II

(Non-legislative acts)

REGULATIONS

COMMISSION IMPLEMENTING REGULATION (EU) 2022/1463

of 5 August 2022

setting out technical and operational specifications of the technical system for the cross-border automated exchange of evidence and application of the 'once-only' principle in accordance with Regulation (EU) 2018/1724 of the European Parliament and of the Council

(Text with EEA relevance)

THE EUROPEAN COMMISSION,

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

Having regard to Regulation (EU) 2018/1724 of the European Parliament and of the Council of 2 October 2018 establishing a single digital gateway to provide access to information, to procedures and to assistance and problem-solving services and amending Regulation (EU) No 1024/2012 ([1]), and in particular Article 14(9) thereof,

Whereas:

(1) Article 14(1) of Regulation (EU) 2018/1724 requires the Commission, in cooperation with Member States, to establish a technical system for the exchange of evidence as required for the online procedures listed in Annex II to that Regulation and the procedures provided for in Directives 2005/36/EC ([2]), 2006/123/EC ([3]), 2014/24/EU ([4]) and 2014/25/EU ([5]) of the European Parliament and of the Council.

(2) The technical and operational specifications of the 'once-only' technical system (OOTS) contained in this Regulation should set out the main components of the architecture of the OOTS, define the technical and operational roles and obligations of the Commission, Member States, evidence requesters, evidence providers and intermediary platforms. Furthermore, these specifications should establish a log system in order to monitor the exchanges and delineate the responsibility for the maintenance, operation and security of the OOTS.

(3) In order to enable the establishment of the OOTS by the date set out in Regulation (EU) 2018/1724, it is envisaged to complement this Regulation by more detailed, non-binding technical design documents drawn up in a consensual manner by the Commission in cooperation with the Member States within the gateway coordination group and in accordance with the Commission's Guidelines for the implementation of the single digital gateway Regulation 2021-2022 work programme. However, where deemed necessary in the light of new technical developments or discussions or differences of opinion within the gateway coordination group, notably on the finalisation of the technical design documents and major design choices, or when the need arises to make certain

([1]) OJ L 295, 21.11.2018, p. 1.
([2]) Directive 2005/36/EC of the European Parliament and of the Council of 7 September 2005 on the recognition of professional qualifications (OJ L 255, 30.9.2005, p. 22).
([3]) Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market (OJ L 376, 27.12.2006, p. 36).
([4]) Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC (OJ L 94, 28.3.2014, p. 65).
([5]) Directive 2014/25/EU of the European Parliament and of the Council of 26 February 2014 on procurement by entities operating in the water, energy, transport and postal services sectors and repealing Directive 2004/17/EC (OJ L 94, 28.3.2014, p. 243).

elements of the technical design documents binding, it will be possible to complement/amend the technical and operational specifications set out in this Regulation in accordance with the examination procedure referred to in Article 37(2) of Regulation (EU) 2018/1724.

(4) In order to reduce the costs of, and the time necessary for, establishing the OOTS, the architecture of the OOTS should, to the extent possible, rely on reusable solutions, be implementation technology neutral and accommodate different national solutions. For example, the OOTS should be able to use the existing national, including central, regional and local level, procedure portals, data services or intermediary platforms, which have been created for national use. The components developed by the Commission should be released under an open software license that promotes reuse and collaboration.

(5) One such reusable solution developed at Union level is the system of eIDAS nodes laid down in Commission Implementing Regulation (EU) 2015/1501 ([6]), which, by enabling the communication with other nodes of the eIDAS network, can process the request for, and the provision of, cross-border authentication of a user. The eIDAS nodes should enable evidence requesters and, where relevant, evidence providers to identify users requesting evidence to be exchanged through the OOTS so that evidence providers can match the identification data to their existing records.

(6) The OOTS should build on the work already done and exploit synergies with other existing systems for the exchange of evidence or information among authorities relevant for the procedures referred to in Article 14(1) of Regulation (EU) 2018/1724, including systems not covered by Article 14(10) of that Regulation. For example, as far as vehicle and driving license register data is concerned, the OOTS should take into account already developed data models and, where feasible, establish technical bridges to facilitate the connection of competent authorities already using other existing networks (RESPER ([7]) or EUCARIS ([8])) to the OOTS for the provision of evidence in the procedures covered by the OOTS. A similar approach should be taken in relation to other systems such as, but not limited to: the Emrex User Group (EUG) ([9]) in the education domain, the Electronic Exchange of Social Security Information (EESSI) under Regulation (EC) No 987/2009 of the European Parliament and of the Council ([10]) in the social security area, the European Criminal Records Information System established by Council Decision 2009/316/JHA ([11]) for the purpose of judicial cooperation and eCertis ([12]) used in public procurement procedures. The cooperation between these systems and the OOTS should be defined on a case-by-case basis.

(7) For the purpose of cross-border authentication of a user, the architecture of the OOTS should be aligned with Regulation (EU) No 910/2014 of the European Parliament and of the Council ([13]). On 3 June 2021, the Commission adopted a Recommendation on a common Union Toolbox for a coordinated approach towards a European Digital Identity Framework ([14]). This Recommendation sets up a structured process for cooperation between Member States, the Commission and, where relevant, private sector operators to work on the technical aspects of the European Digital Identity Framework. In order to ensure the necessary alignment between that

([6]) Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (OJ L 235, 9.9.2015, p. 1).

([7]) Driving licence network set up on the basis of Article 15 of Directive 2006/126/EC of the European Parliament and of the Council of 20 December 2006 on driving licences (OJ L 403, 30.12.2006, p. 18).

([8]) Treaty concerning a European Vehicle and Driving Licence Information System (EUCARIS), adopted in Luxembourg on 29 June 2000.

([9]) Emrex User Group (EUG) is an independent, international network which unites various actors interested in enhancing student data portability; https://emrex.eu/

([10]) Regulation (EC) No 987/2009 of the European Parliament and of the Council of 16 September 2009 laying down the procedure for implementing Regulation (EC) No 883/2004 on the coordination of social security systems (OJ L 284, 30.10.2009, p. 1).

([11]) Council Decision 2009/316/JHA of 6 April 2009 on the establishment of the European Criminal Records Information System (ECRIS) in application of Article 11 of Framework Decision 2009/315/JHA (OJ L 93, 7.4.2009, p. 33).

([12]) https://ec.europa.eu/tools/ecertis/#/homePage

([13]) 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).

([14]) A trusted and secure European e-ID - Recommendation | Shaping Europe's digital future (europa.eu)

process and the OOTS, the Commission should ensure appropriate coordination, in particular through the Synergies and Interoperability Contact Group, between the Cooperation Network established by Commission Implementing Decision (EU) 2015/296 ([15]) and the gateway coordination group.

(8) To ensure the security of the cross-border electronic delivery services for the purposes of the OOTS, Member States should ensure that such services comply with the requirements for electronic registered delivery services, laid down in Article 44 of Regulation (EU) No 910/2014. To that effect, it is appropriate that the OOTS uses eDelivery Access Points to create a network of nodes for secure digital data exchange. In addition to enabling secure cross-border delivery, eDelivery provides metadata service functionalities that may support future versions of the OOTS with larger numbers of secure data exchange nodes. Within that framework, Member States should be able to choose the providers of their eDelivery software.

(9) To ensure flexibility in the application of this Regulation, Member States should be able to decide to have either one or several eDelivery Access Points, as part of the OOTS. A Member State should therefore be able to deploy a single Access Point managing all OOTS-related eDelivery messaging to the evidence requesters or evidence providers through an intermediary platform, where applicable, or, alternatively, to deploy multiple Access Points at any hierarchical level or for specific domains or sectors or geographic levels of its public administrations.

(10) According to Union law, including Directives 2005/36/EC, 2006/123/EC, 2014/24/EU, 2014/25/EU and Regulation (EU) 2018/1724, certain administrative procedures are to be made available to users online. As those procedures and the evidence required are not harmonised under Union law, common services should be established to enable the cross-border exchange of evidence required for these procedures through the OOTS.

(11) Where there is no agreed evidence type that is harmonised across the Union and that all Member States can provide, an evidence broker should help determine which evidence types can be accepted for a particular procedure.

(12) The evidence broker should be based on rule content provided by Member States and should provide an on-line mechanism for Member States to query their information requirements and evidence type sets. The evidence broker should allow Member States to manage and share information about rules relating to types of evidence.

(13) In cases where interoperability is needed between the procedure portal and the data services and the common services, this should be supported by technical design documents.

(14) This Regulation should specify when structured and unstructured pieces of evidence that are required for the procedures listed in Article 14(1) of Regulation (EU) 2018/1724 are considered as lawfully issued in electronic format that allows automatic exchange. Unstructured pieces of evidence issued in an electronic format can be exchanged through the OOTS if they are supplemented by the metadata elements of the OOTS generic metadata model contained in the semantic repository referred to in Article 7(1) of this Regulation. Structured pieces of evidence can be exchanged through the OOTS if they are supplemented by the metadata elements of the OOTS generic metadata model referred to in Article 7(1) of this Regulation and are either in compliance with the OOTS data model for the relevant evidence type as referred to in Article 7(2) of this Regulation or accompanied by a human-readable version.

([15]) Commission Implementing Decision (EU) 2015/296 of 24 February 2015 establishing procedural arrangements for cooperation between Member States on electronic identification pursuant to Article 12(7) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (OJ L 53, 25.2.2015, p. 14).

(15) Member States should be free to determine when they convert pieces of evidence to an electronic format that allows their automated exchange through the OOTS. However, in order to enhance the usefulness of the OOTS for its users and since the use of data models and metadata schemata for both unstructured and structured formats is generally highly recommended, the Commission should support Member States in their efforts to work towards this goal.

(16) In order to avoid duplication, ensure synergies and provide user choice, the development of OOTS data models for structured evidence types and the standardisation of use cases for the provision of credentials in accordance with the structured process foreseen by Commission Recommendation (EU) 2021/946 of 3 June 2021 on a common Union Toolbox for a coordinated approach towards a European Digital Identity Framework ([16]) should be done in close cooperation and alignment with each other as far as evidence covered by Article 14 of Regulation (EU) 2018/1724 is concerned, including by identifying common use cases. The alignment of the OOTS data models and the standardised use cases under the aforementioned Commission Recommendation should allow users to rely on alternative means for the provision of evidence covered by Article 14 of Regulation (EU) 2018/1724 either independently of or in combination with the OOTS. When changes are made to the data models and metadata schemata for pieces of evidence contained in the semantic repository, Member States should be given 12 months from the adoption of any update to apply any changes to the pieces of evidence concerned.

(17) To minimise the amount of data exchanged, in the case of structured evidence, if only a subset of data is requested in the evidence request, the evidence provider or an intermediary platform, where applicable, could enable automated filtering of the data and, where necessary to the transfer, transformation of the data on behalf of the responsible data controller so that only the requested data are exchanged.

(18) Where Member States manage national registries and services that play the same or an equivalent role as the data service directory or the evidence broker, they should not be required to duplicate their work by contributing to the relevant common services. However, in such a case they should ensure that their national services are connected to the common services in such a way that they can be used by other Member States. Alternatively, those Member States should be able to copy the relevant data from the national registries or services to the data service directory or evidence broker.

(19) In the 2017 Tallinn Declaration on eGovernment ([17]), Member States reaffirmed their commitment to progress in linking up their public eServices and implement the once-only principle in order to provide efficient and secure digital public services that will make citizens and businesses lives easier. The 2020 Berlin Declaration on Digital Society and Value-Based Digital Government ([18]), built on the principles of user centricity and user-friendliness, and set out further key principles on which digital public services should be based, including trust and security in digital government interactions and digital sovereignty and interoperability. This Regulation should implement those commitments by putting users at the centre of the system and requiring that users should be informed about the OOTS, its steps and the consequences of using the system.

(20) It is important that an appropriate system is in place to allow users to identify themselves for the purposes of the exchange of evidence. The only mutual recognition framework for national electronic identification means at Union level is set out in Regulation (EU) No 910/2014. Electronic identification means issued under electronic identification schemes notified in accordance with that Regulation should therefore be used by evidence requesters to authenticate the identity of a user before the user explicitly requests the use of the OOTS. Where the identification of the relevant evidence provider requires the provision of attributes beyond the mandatory attributes of the minimum data set listed in the Annex to Implementing Regulation (EU) 2015/1501, such additional attributes should also be requested from the user by the evidence requester and provided to the evidence provider or intermediary platform, where applicable, as part of the evidence request.

([16]) OJ L 210, 14.6.2021, p. 51.

([17]) Signed on 6 October 2017, https://digital-strategy.ec.europa.eu/en/news/ministerial-declaration-egovernment-tallinn-declaration

([18]) Signed on 8 December 2020; https://digital-strategy.ec.europa.eu/en/news/berlin-declaration-digital-society-and-value-based-digital-government

(21) Some of the procedures listed in Article 14(1) of Regulation (EU) 2018/1724 require that evidence can be requested on behalf of a legal or natural person. For example, certain procedures are relevant for businesses and entrepreneurs should therefore be able to request the exchange of evidence either on their own behalf or through a representative. Regulation (EU) No 910/2014 provides a trusted legal framework for electronic identification means issued for legal persons or for natural persons representing legal persons. The mutual recognition of national electronic identification means under that Regulation applies to these cases of representation. This Regulation should therefore rely on Regulation (EU) No 910/2014, and any implementing acts adopted on its basis, for the identification of users in cases of representation. The gateway coordination group and its subgroups should cooperate closely with the governance structures established under Regulation (EU) No 910/2014 to help develop solutions for powers of representation and mandates. Given the reliance of some of the procedures covered by the OOTS on the framework created by Regulation (EU) No 910/2014, pieces of evidence requested by representatives should also be able to be processed through the OOTS when and to the extent to which these solutions will have been found.

(22) In order to reduce the time and cost to implement the OOTS, and to benefit from each other's implementation experience, the Commission should support Member States and foster collaboration between them on the development of reusable technical solutions and components that can be used to implement national procedure portals, preview spaces and data services.

(23) In order to guarantee that users retain control over their personal data at all times while using the OOTS as provided for in Regulation (EU) 2018/1724, the OOTS should allow users to express their decision in relation to these data in two instances. First, it should be ensured that users receive sufficient information to enable them to make an informed and explicit request to process their request for evidence through the OOTS in accordance with Article 14(3), point (a), and Article 14(4), of Regulation (EU) 2018/1724. It should then ensure that they can view the evidence to be exchanged in a secure preview space before deciding whether or not to proceed with the exchange of evidence in accordance with Article 14(3), point (f), of Regulation (EU) 2018/1724, except in the cases referred to in Article 14(5) of that Regulation.

(24) Responsibility for the establishment of the OOTS is shared between Member States and the Commission and the gateway coordination group should therefore play a central role in the governance of the system. In view of the technical nature of its work and in order to facilitate implementation in existing national systems of technical design documents, the work of the gateway coordination group should be supported and prepared by experts coming together in one or several sub-groups created in accordance with its rules of procedure. The functioning of this OOTS governance should be assessed in the report that the Commission is required to submit to the European Parliament and to the Council by 12 December 2022 pursuant to Article 36 of Regulation (EU) 2018/1724.

(25) To ensure a quick reaction to any possible incidents and downtimes which may affect the functioning of the OOTS, the Member States and the Commission should establish a network of technical support contact points. In order to ensure the proper functioning of the OOTS, those technical support contact points should have the powers and sufficient human and financial resources to enable them to carry out their tasks.

(26) To ensure an efficient functioning and maintenance of the OOTS, the responsibilities for its different components should be clearly distributed. The Commission, as the owner and operator of the common services, should be responsible for their maintenance, hosting and security. Each Member State should be responsible for ensuring maintenance and the security of those components of the OOTS that they own and for which they are responsible, such as eIDAS nodes, eDelivery Access Points or national registries, in accordance with the relevant Union and national law.

(27) In order to ensure appropriate protection of personal data, as required by Regulation (EU) 2016/679 of the European Parliament and of the Council ([19]), this Regulation should specify the role of Member States, in particular that of the respective competent authorities in their capacity as evidence requester or evidence provider, and of the intermediary platforms, where applicable, in relation to the personal data contained in the evidence that is exchanged through the OOTS.

(28) To ensure that the common services are protected against potential threats that harm the confidentiality, integrity or availability of the Commission's communication and information systems Commission Decision (EU, Euratom) 2017/46 ([20]) should apply to these services.

(29) Article 14(1) to (8) and (10) of Regulation (EU) 2018/1724 apply from 12 December 2023. Therefore, the requirements laid down in this Regulation should also apply from that date.

(30) 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 ([21]) and delivered Formal Comments on 6 May 2021 ([22]).

(31) The measures provided for in this Regulation are in accordance with the opinion of the Single Digital Gateway Committee,

HAS ADOPTED THIS REGULATION:

SECTION 1

GENERAL PROVISIONS

Article 1

Definitions

For the purposes of this Regulation, the following definitions shall apply:

(1) 'once-only technical system' ('OOTS') means the technical system for the cross-border automated exchange of evidence referred to in Article 14(1) of Regulation (EU) 2018/1724;

(2) 'evidence provider' means a competent authority as referred to in Article 14(2) of Regulation (EU) 2018/1724 that lawfully issues structured or unstructured evidence;

(3) 'evidence requester' means a competent authority responsible for one or more of the procedures referred to in Article 14(1) of Regulation (EU) 2018/1724;

(4) 'eDelivery Access Point' means a communication component that is part of the eDelivery electronic delivery service based on technical specifications and standards, including the AS4 messaging protocol and ancillary services developed under the Connecting Europe Facility Programme and continued under the Digital Europe Programme, to the extent that these technical specifications and standards overlap with the ISO 15000-2 standard;

([19]) 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).

([20]) Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission (OJ L 6, 11.1.2017, p. 40).

([21]) 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).

([22]) https://edps.europa.eu/data-protection/our-work/publications/formal-comments/draft-commission-implementing-regulation-4_en

(5) 'eIDAS node' means a node as defined in Article 2, point (1), of Implementing Regulation (EU) 2015/1501 and complying with the technical and operational requirements laid down in and on the basis of that Regulation;

(6) 'intermediary platform' means a technical solution acting in its own capacity or on behalf of other entities such as evidence providers or evidence requesters, depending on the administrative organisation of Member States in which the intermediary platform operates, and through which evidence providers or evidence requesters connect to the common services referred to in Article 4(1) or to evidence providers or evidence requesters from other Member States;

(7) 'data service directory' means a registry containing the list of evidence providers and the evidence types they issue together with the relevant accompanying information;

(8) 'evidence broker' means a service allowing an evidence requester to determine which evidence type from another Member State satisfies the evidence requirement for the purposes of a national procedure;

(9) 'electronic identification means' means a material and/or immaterial unit, containing person identification data and which is used for authentication for an online service;

(10) 'semantic repository' means a collection of semantic specifications, linked to the evidence broker and the data service directory, composed of definitions of names, data types and data elements associated with specific evidence types to ensure mutual understanding and cross-lingual interpretation for evidence providers, evidence requesters and users, when exchanging evidence through the OOTS;

(11) 'technical design documents' means a set of detailed and non-binding technical documents, drawn up by the Commission in cooperation with Member States in the framework of the gateway coordination group referred to in Article 29 of Regulation (EU) 2018/1724 or any sub-groups referred to in Article 19 of this Regulation, which includes but is not limited to, a high-level architecture, exchange protocols, standards and ancillary services that support the Commission, Member States, evidence providers, evidence requesters, intermediary platforms and other entities concerned in establishing the OOTS in compliance with this Regulation;

(12) 'data service' means a technical service through which an evidence provider handles the evidence requests and dispatches evidence;

(13) 'data model' means an abstraction that organises elements of data, standardises how they relate to one another and specifies the entities, their attributes and the relationship between such entities;

(14) 'preview space' means a functionality that enables the user to preview the requested evidence as referred to in Article 15(1), point (b)(ii);

(15) 'structured evidence' means any evidence in electronic format required for the procedures listed in Article 14(1) of Regulation (EU) 2018/1724 that is organised in predefined elements or fields that have a specific meaning and technical format allowing for processing by software systems, supplemented by the metadata elements of the OOTS generic metadata model referred to in Article 7(1) of this Regulation and either in compliance with the OOTS data model for the relevant evidence type as referred to in Article 7(2) of this Regulation, or accompanied by a human-readable version;

(16) 'unstructured evidence' means evidence in electronic format required for the procedures listed in Article 14(1) of Regulation (EU) 2018/1724 that is not organised in predefined elements or fields that have specific meaning and technical format, but is supplemented by the metadata elements of the OOTS generic metadata model referred to in Article 7(1) of this Regulation;

(17) 'evidence type' means a category of structured or unstructured evidence with a common purpose or content;

(18) 'incident' means a situation where the OOTS is not performing, fails to transmit the evidence or transmits evidence that has not been requested, or where the evidence has changed or been disclosed during the transmission, as well as any breach of security referred to in Article 29;

(19) 'procedure portal' means a webpage or a mobile application where a user can access and complete an online procedure referred to in Article 14(1) of Regulation (EU) 2018/1724.

Article 2

Structure of the OOTS

The OOTS shall consist of the following:

(a) the procedure portals of evidence requesters and the data services of evidence providers;

(b) intermediary platforms, where relevant;

(c) the preview spaces referred to in Article 15(1), point (b)(ii);

(d) the national registries and services referred to in Article 8, where relevant;

(e) eIDAS nodes for user authentication and identity matching;

(f) eDelivery Access Points;

(g) the common services referred to in Article 4(1);

(h) the integration elements and interfaces required to connect the components referred to in points (a) to (g).

SECTION 2

SERVICES OF THE OOTS

Article 3

eIDAS nodes and eDelivery Access Points

1. Member States shall ensure that evidence requesters are connected to an eIDAS-node to enable user authentication pursuant to Article 11, either directly or through an intermediary platform.

2. Member States shall ensure that eDelivery Access Points are installed, configured and integrated in the procedure portals of evidence requesters, in the data services of evidence providers and in intermediary platforms.

3. Member States may choose the number of eDelivery Access Points they use for the OOTS.

Article 4

Common services

1. The Commission in cooperation with Member States shall establish the following services of the OOTS ('common services'):

(a) the data service directory referred to in Article 5;

(b) the evidence broker referred to in Article 6;

(c) the semantic repository referred to in Article 7.

2. Member States shall ensure the technical connection between the procedure portals of evidence requesters, directly or through intermediary platforms, with the common services and the proper registration of their data services in the common services. In implementing these connections, Member States shall be guided by the descriptions contained in the technical design documents.

3. Member States shall ensure that only evidence requesters are connected, directly or through intermediary platforms, to the common services and that only evidence requesters and evidence providers can use the OOTS. Member States shall check the functioning of the connections to the common services at regular intervals.

Article 5

Data service directory

1. Without prejudice to Article 8 of this Regulation, Member States shall ensure that all evidence providers and evidence types issued by them that are relevant for the online procedures referred to in Article 14(1) of Regulation (EU) 2018/1724 are registered in the data service directory.

2. The Commission shall be responsible for the development and maintenance of interfaces allowing national coordinators referred to in Article 28 of Regulation (EU) 2018/1724, competent authorities, intermediary platforms where applicable, and the Commission, each within the scope of their responsibilities and the limits of the access rights defined by the Commission, to:

(a) register, de-register and carry out any other updates of information contained in the data service directory;

(b) manage the access rights of persons who are authorised to make registrations and changes to the registered data.

The Commission shall ensure that national coordinators, competent authorities and intermediary platforms can choose between graphical user interfaces for authorised persons and programmatic interfaces for automated uploads.

3. Member States shall ensure that each type of evidence registered in the data service directory is accompanied by:

(a) the level of assurance of the electronic identification means notified by Member States in accordance with Regulation (EU) No 910/2014; and

(b) where applicable, additional attributes, specified in order to facilitate the identification of the relevant evidence provider and that go beyond the mandatory attributes of the minimum data set laid down in accordance with Implementing Regulation (EU) 2015/1501, exchanged using the electronic identification means notified in accordance with Regulation (EU) No 910/2014, required for its exchange through the OOTS.

4. The data service directory shall make a clear distinction between the additional attributes referred to in paragraph 3, point (b), of this Article and the attributes exchanged using the electronic identification means notified in accordance with Regulation (EU) No 910/2014 referred to in Article 13(1), point (f), of this Regulation.

5. The level of assurance referred to in paragraph 3, point (a), required for cross-border users shall not exceed the level of assurance required for non-cross-border users.

6. Member States shall ensure that the information in the data service directory is kept up to date.

Article 6

Evidence broker

1. The evidence broker shall allow evidence requesters to determine which evidence types issued in other Member States correspond to the evidence types required in the context of procedures for which that evidence requester is competent.

2. Member States shall, through the interface referred to in Article 5(2), complement the list of evidence types in the data service directory as referred to in Article 5(1) with the facts or compliance with procedural requirements they prove, possibly jointly with other evidence types, if needed. Member States shall ensure that this information is accurate and kept up to date.

3. The Commission shall be responsible for the development and maintenance of interfaces that allow national coordinators, competent authorities, intermediary platforms where applicable, and the Commission, each within the scope of their responsibilities and the limits of the access rights defined by the Commission, to:

(a) add, change and update the information referred to in paragraph 2;

(b) manage the access rights of persons who are authorised to make additions and changes to the registered information.

The Commission shall ensure that national coordinators, competent authorities and intermediary platforms can choose between graphical user interfaces for authorised persons and programmatic interfaces for automated uploads.

4. The Commission shall facilitate the mapping of the evidence types issued in one Member State to facts or compliance with procedural requirements that have to be proved in a procedure in another Member State by structuring the discussion and organising the work in the relevant sub-group referred to in Article 19. The sub-group shall set out a formal domain-specific language, whenever possible referencing relevant international standards, and propose that language to the gateway coordination group in accordance with Article 18, point (f).

Article 7

Semantic repository and data models

1. The semantic repository shall provide access to the OOTS generic metadata model, which is designed to display metadata that uniquely identify the evidence and the evidence provider and which includes additional fields designed to display the metadata referred to in Article 13(1), points (a), (b) and (c).

2. For the types of structured evidence agreed in the gateway coordination group, the semantic repository shall contain an OOTS data model consisting of at least the following components:

(a) a representation of that data model with:

  (i) a visual data model diagram; and

  (ii) a textual description of all the entities of the data model, consisting of a definition and the list of the attributes of the entity; and, for each attribute, the expected type (e.g. Boolean, Identifier, Date), a definition, the cardinality and the optional usage of a code list;

(b) distributions in XML based on XML schema definition (XSD), or an equivalent format, complemented by other widely used serialisation formats, where feasible;

(c) code lists to ensure the automated processing of evidence, available in a structured format;

(d) a mechanism for conversion into a human-readable format, such as XSLT or equivalent.

3. For each type of evidence, the semantic repository shall offer version control and a change log to keep track of different versions.

4. The semantic repository shall contain a methodology for developing new OOTS data models for evidence types exchanged through the OOTS, consisting of examples and learning materials.

5. Schedules for updates and adaptations to the OOTS generic metadata models and the OOTS data models shall be regularly discussed by Member States and the Commission in the framework of one of sub-groups of the gateway coordination group referred to in Article 19 and adopted by the gateway coordination group. The evidence providers or intermediary platforms, where applicable, shall apply those updates and adaptations at the latest 12 months after their publication in the semantic repository.

6. The Commission shall provide Member States with an IT tool which will help them to verify the compliance of the evidence with the OOTS generic metadata model and the OOTS data models.

7. The Commission shall make the semantic repository publicly available on a dedicated Commission website.

Article 8

National registries and services

1. Member States that have national registries or services that are equivalent to the data service directory or evidence broker may choose not to register evidence providers, the types of evidence they issue and the facts or compliance with procedural requirements they prove, possibly jointly with other evidence types, and the level of assurance of the electronic identification means required to access each type of evidence as provided for in Articles 5 and 6. In such a case, they shall instead do one of the following:

(a) allow other Member States to search their national registries for the information referred to under this paragraph;

(b) copy the information referred to under this paragraph from the national registries or services to the data service directory or evidence broker.

2. When implementing paragraph 1, Member States shall be guided by the descriptions contained in the technical design documents.

SECTION 3

EVIDENCE REQUESTERS

Article 9

Explanation to users

1. Evidence requesters shall ensure that their procedure portals contain an explanation of the OOTS and its features, including the information that:

(a) the use of the OOTS is voluntary;

(b) users have the option to preview the evidence in the preview space referred to in Article 15(1), point (b)(ii), and decide whether or not to use it for the procedure;

(c) users can act on their own behalf or be represented by another legal or natural person, when and to the extent to which solutions for representation, in accordance with Regulation (EU) No 910/2014 and any implementing acts adopted on its basis, have been found.

The information referred to in point (b) of the first subparagraph of this paragraph shall not be required in the case of the procedures referred to in Article 14(5) of Regulation (EU) 2018/1724.

2. The obligation to provide explanations referred to in paragraph 1 of this Article shall be without prejudice to the obligation to provide the data subjects with the information referred to in Articles 13 and 14 of Regulation (EU) 2016/679.

Article 10

Evidence type selection

1. Evidence requesters shall give users the possibility to request the types of evidence that correspond, based on the information registered in the evidence broker, to types that would be acceptable under the applicable law in the relevant procedure by direct submission, provided that evidence providers make these types of evidence available through the OOTS in accordance with Article 5(1).

2. If multiple pieces of evidence can be requested the evidence requester shall ensure that users can select all, a sub-set of, or a specific type of, the evidence.

Article 11

User authentication

1. Evidence requesters shall rely on electronic identification means that have been issued under an electronic identification scheme that has been notified in accordance with Regulation (EU) No 910/2014 to authenticate the users, acting either on their own behalf or through a representative, when and to the extent to which solutions for representation in accordance with Regulation (EU) No 910/2014 and any implementing acts adopted on its basis, have been found.

2. Once the user has selected the type of evidence to be exchanged through the OOTS, the evidence requesters shall inform users:

(a) where applicable, of any additional attributes referred to in Article 5(3), point (b), of this Regulation that they are to provide; and

(b) that they will be redirected to the relevant evidence provider, evidence providers or, where applicable, intermediary platform or platforms, to preview the selected evidence.

3. Where preview is not required in accordance with Article 14(5) of Regulation (EU) 2018/1724, paragraph 2, point (b), of this Article shall not apply. In that case the evidence provider, evidence providers or, where applicable, intermediary platform or platforms may ask the evidence requester to redirect the user to reidentify and reauthenticate for the purpose of identity and evidence matching. The user may choose not to be redirected. In that case, the evidence requester shall inform the user that the process of identity and evidence matching carried out by the evidence provider might not result in a match as referred to in Article 16 of this Regulation.

Article 12

Explicit request

The evidence requester shall, in addition to the information referred to in Article 9, provide the user with the following:

(a) the name(s) of the evidence provider(s);

(b) the evidence type(s) or data fields to be exchanged.

This Article is without prejudice to the situations where the use of the OOTS is permitted without an explicit request in accordance with Article 14(4) of Regulation (EU) 2018/1724.

Article 13

Evidence request

1. The evidence requester shall ensure that the evidence request is transmitted to the evidence provider or intermediary platform, where applicable, and contains the following information:

(a) the unique identifier of the request;

(b) the evidence type that is requested;

(c) date and time when the explicit request was made;

(d) identification of the procedure for which the evidence is required;

(e) name and metadata that uniquely identifies the evidence requester and intermediary platform, where applicable;

(f) the attributes of the user, or the user and the representative where applicable, exchanged using the electronic identification means referred to in Article 11(1);

(g) the level of assurance, as defined in Regulation (EU) No 910/2014, of the electronic identification means used by the user;

(h) the additional attributes, referred to in Article 5(3), point (b), provided by the user for the purpose of the request;

(i) the identification of the evidence provider as registered in the data service directory;

(j) whether the explicit request of the user was required in accordance with Article 14(4) of Regulation (EU) 2018/1724;

(k) whether the possibility of previewing the evidence is required in accordance with Article 14(5) of Regulation (EU) 2018/1724.

2. The evidence requester shall make a clear distinction between the additional attributes referred to in paragraph 1, point (h), and the attributes referred to in paragraph 1, point (f).

Article 14

User redirection to the evidence provider

1. Without prejudice to the procedures referred to in Article 14(5) of Regulation (EU) 2018/1724, evidence requesters shall ensure that users, after selecting the evidence to be exchanged through the OOTS in the procedure portal in accordance with Article 10 of this Regulation and stating their explicit request in accordance with Article 12 of this Regulation are redirected to the evidence provider, evidence providers or intermediary platform or platforms, where applicable, to exercise the option to preview the evidence.

2. For the procedures referred to in Article 14(5) of Regulation (EU) 2018/1724, users can be redirected to the evidence provider, evidence providers or intermediary platform or platforms, where applicable, in accordance with Article 11(3) of this Regulation.

SECTION 4

EVIDENCE PROVIDERS

Article 15

Role in the exchange of evidence

1. Member States shall ensure that, for the purpose of the evidence exchange through the OOTS, the evidence providers or intermediary platforms, where applicable, shall use application services capable of the following:

(a) receiving and interpreting evidence requests delivered by an eDelivery Access Point, which shall be considered as the input to the data services;

(b) subject to successful identification and authentication in accordance with Article 16 of this Regulation:

  (i) retrieving any pieces of evidences matching the request;

  (ii) except in the case of the procedures referred to in Article 14(5) of Regulation (EU) 2018/1724, allow users to specify which of these pieces of evidence they wish to preview and give them the possibility to preview the pieces thus specified in a preview space;

  (iii) allow users to indicate which, if any, of the matching pieces of evidence should be returned to the evidence requester for use in the procedure;

(c) returning evidence responses to the evidence requester through an eDelivery Access Point, subject to the user's decision to use the evidence in the procedure following the possibility to preview it, except in the case of the procedures referred to in Article 14(5) of Regulation (EU) 2018/1724, error reports, including in the situation referred to in Article 16(3), point (a), of this Regulation, or reports concerning evidence in the process of being converted.

2. If an evidence response is returned, it shall include the requested evidence and be accompanied by:

(a) metadata that uniquely identifies the evidence response;

(b) metadata that uniquely identifies the evidence request;

(c) metadata that indicates the date and time at which the response was generated;

(d) metadata that uniquely identifies the evidence and the evidence provider;

(e) where structured evidence does not comply with the OOTS data model relevant for the evidence type concerned, a human-readable version of the evidence.

3. The evidence response may also include the metadata that uniquely identifies the language or languages of the requested evidence.

4. If an error report is returned, it shall include metadata that uniquely identifies the evidence request, the date and time at which it was generated and a description of the error that occurred.

5. Where evidence is not yet available for exchange through the OOTS but in the process of being converted to structured or unstructured evidence as defined in Article 1, points (16) and (17), a report as referred to in paragraph 1, point (c), of this Article shall be returned. That report shall include metadata that uniquely identifies the evidence request, the date and time at which it was generated and a message that the evidence concerned is in the process of being converted to structured or unstructured evidence as defined in Article 1, points (16) and (17), and will be ready for the transmission through the OOTS in the future. The evidence provider shall include in the report the preliminary date and time for when the evidence will be available.

Article 16

Identity and evidence matching

1. Evidence providers or intermediary platforms, where applicable, may require users to reidentify and reauthenticate for the purpose of identity and evidence matching, including by providing additional attributes.

2. Evidence providers, or intermediary platforms, where applicable, shall ensure that evidence is only exchanged through the OOTS if the identity attributes of the user, and of the representative where applicable, exchanged using the electronic identification means referred to in Article 11(1) and additional attributes as referred to in Article 11(2), point (a) and provided by the user to facilitate identification by the relevant evidence provider, match the attributes held by them.

3. Where the process of identity and evidence matching does not result in a match or the identity matching generates two or more results, the user or the representative where applicable shall not be allowed to preview the requested evidence and the evidence shall not be exchanged. In the absence of no such match:

(a) an error message shall be sent to the evidence requester;

(b) the user shall receive an automated message explaining that the evidence cannot be provided.

SECTION 5

LOG SYSTEM OF THE OOTS

Article 17

Log system

1. For each evidence request transmitted through the OOTS, the evidence requester, evidence provider(s) or intermediary platform(s), where applicable, shall log the following elements:

(a) the evidence request referred to in Article 13(1);

(b) the information included in the evidence response, with the exception of the evidence itself, or error report referred to in Article 15(1), point (c), and Article 16(3), point (a);

(c) the eDelivery event data related to any of the following:

(i) exchange of evidence requests;

(ii) evidence responses;

(iii) error reports.

2. For each piece of evidence exchanged through the OOTS, the evidence provider or intermediary platform, where applicable, shall log the decision of the user after previewing the evidence to approve, or not, the use of the piece of evidence for the procedure, or where applicable the fact that the user leaves the preview space or procedure portal without making a specific decision.

3. The Commission and, in situations referred to in Article 8(1), point (a), the relevant Member States, shall log all interactions with the common services referred to in Article 4(1).

4. Without prejudice to longer retention periods required under national law for the logs referred to in paragraphs 1, 2 and 3 for the purposes of the OOTS or for other purposes, the Commission and the evidence requesters, evidence providers or intermediary platforms, where applicable, shall keep those logs for a period of 12 months.

5. In case of suspicion of incidents and for the purposes of audits and random checks of security performed within their respective areas of responsibility referred to in Article 26, the evidence requesters, evidence providers and intermediary platforms, where applicable, shall make available to each other on request the relevant logs referred to in paragraphs 1 and 2 of this Article through the technical support dashboard referred to in Article 22. For those same purposes and in the same manner, Member States and the Commission, where applicable, shall make available to the relevant evidence requesters, evidence providers and intermediary platforms, where applicable, the relevant logs referred to in paragraph 3 of this Article.

SECTION 6

GOVERNANCE OF THE OOTS

Article 18

Gateway coordination group

The Commission, in cooperation with Member States in the framework of the gateway coordination group established by Article 29 of Regulation (EU) 2018/1724, shall:

(a) oversee the establishment and launch of the OOTS in line with Article 31(3) of this Regulation;

(b) set priorities for further developments and improvements to the OOTS;

(c) determine an indicative schedule for the regular updates to, and maintenance and adaptation of, the technical design documents;

(d) recommend changes in the technical design documents;

(e) organise peer reviews to promote exchanges of experience and good practice between Member States on the application of this Regulation by Member States;

(f) approve or reject operational modalities submitted by any of the sub-groups established in accordance with the rules of procedure of the gateway coordination group, and, if needed, give specific guidance, and supervise their work.

Article 19

Sub-groups of the gateway coordination group

1. To ensure a coordinated development and operation of the OOTS, the sub-groups referred to in Article 18, point (f), shall discuss and where necessary draw up proposals of the operational modalities to be submitted to the gateway coordination group on the following areas, in particular:

(a) standardisation of OOTS data models;

(b) evidence mapping;

(c) review, maintenance and interpretation of the technical design documents;

(d) operational governance, in particular operational arrangements and service level agreements;

(e) security of the OOTS, including the drawing up of risk management plans to identify risks, assess their potential impact and plan appropriate technical and organisational responses in case of incidents;

(f) testing and deployment of the OOTS components, including interoperability between the national components of the OOTS referred to in Article 2, points (a) to (f) and (h), and the common services referred to in Article 4(1).

The operational modalities shall include drawing up and proposing standards necessary for interoperability in the respective areas of the sub-groups, following international standards whenever possible. Once approved by the gateway coordination group, these standards shall be included in technical design documents.

2. The sub-groups shall adopt their proposals for operational modalities by consensus whenever possible. Where it appears that consensus cannot be reached, the chair may decide, if it is supported by the simple majority of the members of the subgroup present at the meeting, that a proposal of the sub-group can be submitted to the gateway coordination group.

SECTION 7

TECHNICAL SUPPORT

Article 20

Commission single point of contact for technical support

1. The Commission shall designate a single point of contact for technical support ensuring operation and maintenance of the common services referred to in Article 4(1).

2. The single point of contact for technical support shall liaise with other relevant Commission contact points and coordinate the resolution of problems with eDelivery Access Points or eIDAS nodes.

3. The Commission shall ensure that its single point of contact for technical support is organised in a way which allows it to perform its tasks in all circumstances and to react at short notice.

Article 21

National single point of contact for technical support

1. Each Member State shall designate a single point of contact for technical support to ensure operation and maintenance of the relevant components of the OOTS for which they are responsible pursuant to Section 9.

2. The single points of contact for technical support shall:

(a) provide expertise and advice to evidence providers and evidence requesters for all technical problems encountered in relation to the operation of the OOTS and, where necessary, liaise with the Commission technical contact point and with other national technical support contact points;

(b) investigate and solve any possible downtimes of the eDelivery Access Points, possible security breaches and other incidents;

(c) inform the technical support contact points of any activities that might result in a breach or a suspected breach of the security of the electronic systems.

3. When informed by an evidence provider about doubts as to the lawfulness of one or several evidence requests, the single point of contact for technical support shall:

(a) review evidence requests or samples of evidence requests transmitted from the same evidence requester in the past;

(b) use the technical support dashboard referred to in Article 22 to ask the single point of contact for technical support designated by the Member State of the evidence requester to transmit logs of selected exchanges referred to in Article 17;

(c) bring the issue to the attention of the national coordinator if the problem persists.

4. Member States shall ensure that their respective single point of contact for technical support is organised in a way which allows it to perform its tasks in all circumstances and is able to react at short notice.

Article 22

Technical support dashboard

1. The Commission shall establish a dashboard to facilitate the communication between all technical support contact points.

2. Member States and the Commission shall record in the dashboard the contact details of the technical support contact points and keep it updated.

3. The contact points shall, through the dashboard:

(a) report any incident considered to be substantial;

(b) report any temporary or permanent measures undertaken following incidents;

(c) request from the relevant technical support contact points the logs of selected exchanges in the cases referred to in Article 17(5) and, in case of doubt, as to the lawfulness of the evidence request referred to in Article 21(3);

(d) request any other assistance needed in case of incidents.

4. The national coordinators and the chair of the gateway coordination group shall have access to the dashboard.

5. The Commission and the national coordinators shall use the dashboard to provide information referred to in Article 27 and Article 28(2).

SECTION 8

COOPERATION WITH OTHER GOVERNANCE STRUCTURES

Article 23

Scope of the cooperation

The Commission, together with the gateway coordination group and its sub-groups, shall cooperate with relevant governance structures established by Union law or international agreements in areas relevant for the OOTS in order to achieve synergies and to reuse, to the extent possible, the solutions developed in those other fora.

SECTION 9

RESPONSIBILITY FOR MAINTENANCE AND OPERATION OF COMPONENTS OF THE OOTS

Article 24

Responsibilities of the Commission

The Commission shall be the owner of the common services and the technical support dashboard and responsible for their development, availability, monitoring, updating, maintenance and hosting.

Article 25

Responsibilities of Member States

With respect to the respective national components of the OOTS referred to in Article 2, points (a) to (f) and (h), each Member State shall be considered as the owner and responsible for the establishment, where applicable, and the development, availability, monitoring, updating, maintenance and hosting.

Article 26

Changes and updates

1. The Commission shall inform Member States of changes and updates to the common services.

2. Member States shall inform the Commission of changes and updates to the components under their responsibility that may have repercussions on the functioning of the OOTS.

3. Information on critical updates shall be provided without undue delay. In the case of other, non-critical updates that are likely to affect OOTS components that are owned by other Member States or the common services, the lead time shall be decided by the gateway coordination group on the basis of a proposal from the relevant sub-group.

Article 27

Availability of OOTS

1. The OOTS operating time frame shall be 24 hours a day/7 days a week, with an availability rate of the eDelivery access points, preview spaces and common services of at least 98 % excluding maintenance scheduled in accordance with paragraph 2 of this Article. The service level targets of the remaining OOTS components shall be specified in the service level agreements referred to in Article 19(1), point (d).

2. Member States and the Commission shall notify the scheduled maintenance activities related to the relevant components of the OOTS 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 infrastructure computer room maintenance that may cause up to 6 days unavailability period per year.

To the extent possible, maintenance operations shall be planned outside working hours.

3. Where Member States have fixed weekly service windows, they shall inform the Commission of the time and day when such fixed weekly windows are planned. Without prejudice to the obligations set out in paragraph 2, points (a), (b) and (c), if Member States systems become unavailable during such a fixed window, Member States are exempted from the obligation to notify the Commission on each occasion.

4. In the case of unexpected technical failure of the Member States OOTS components, the relevant Member State shall inform the other Member States and the Commission without delay of their unavailability, and, if known, of the projected resuming of the functioning of the components.

5. In the case of unexpected failure of the common services, the Commission shall inform Member States without delay of the unavailability of one or more common services, and if known, of the projected resuming of the service.

6. The notifications referred to in this Article shall be made through the technical support dashboard referred to in Article 22.

SECTION 10

SECURITY

Article 28

Security of common services and national components

1. The Commission shall ensure the security of the common services referred to in Article 4(1) and the integration elements and interfaces referred to in Article 2, point (h), for which it is responsible.

2. Member States shall ensure the security of the national components of the OOTS and the integration elements and interfaces referred to in Article 2, point (h), for which they are responsible.

3. For the purposes referred to in paragraphs 1 and 2, Member States and the Commission shall, at least, and each for the component for which they are responsible, take the necessary measures to:

(a) prevent any unauthorised person from having access to components for which they are responsible;

(b) prevent the entry of data and any consultation, modification or deletion of data by unauthorised persons;

(c) detect any of the activities referred to in points (a) and (b); and

(d) ensure logging of security events in line with recognised international security standards for information technology.

4. Member States shall ensure, in particular:

(a) that the connections they operate into and out of the eDelivery Access Points and all internal communication between different national authorities fulfil at least the same level of security requirements as the eDelivery electronic delivery service to protect the security and confidentiality of the exchange and the integrity of evidence exchanged through the OOTS;

(b) the non-repudiation of origin of the evidence request transmitted from the access point of the evidence requester, and of the evidence response exchanged or error message transmitted from the access point of the evidence provider.

5. In accordance with paragraph 4, the Member State of the evidence provider in any given exchange of evidence shall be responsible for the quality, confidentiality, integrity and availability of the requested evidence until it reaches the eDelivery Access Point of the evidence requester or an intermediary platform, where applicable. The Member State of the evidence requester in any given exchange of evidence shall be responsible for the confidentiality and integrity of the requested evidence from the moment it reaches its eDelivery Access Point.

6. Member States and the Commission shall ensure the confidentiality, integrity and availability of the logs referred to in Article 17(1), (2) and (3) through appropriate and proportionate security measures, each for the logs that they have recorded.

Article 29

Monitoring of the electronic systems

1. Member States and the Commission shall conduct regular checks on the components of the OOTS for which they are responsible.

2. The single points of contact for technical support referred to in Articles 20 and 21 shall use the technical support dashboard referred to in Article 22 to inform each other of problems discovered during the checks that might result in a breach or a suspected breach of the security of the OOTS.

Article 30

Administration management system

The Commission shall set up an administration management system to manage the authentication and authorisation rules for validating the identification data for the purposes of allowing access to the common services and the technical support dashboard.

SECTION 11

FINAL PROVISIONS

Article 31

Testing of the OOTS

1. Member States and the Commission shall, in the framework of the gateway coordination group, adopt a testing schedule and a set of indicators according to which testing results can be measured and considered as positive.

2. The Commission shall provide testing services that Member States can use to test the conformity of technical solutions with the indicators referred to in paragraph 1.

3. Member States and the Commission shall test the functioning of each of the OOTS components and verify that they can function properly according to the indicators referred to in paragraph 1. Only those components of the OOTS for which the tests yield positive results shall be made available for users.

Article 32

Commission assistance

The Commission shall provide a team of experts as part of the Commission technical support contact point to assist national technical support contact points, and national coordinators in all aspects related to the functioning of the OOTS from a technical point of view, in particular:

(a) providing guidelines;

(b) organising workshops and demonstrations;

(c) answering individual questions.

Article 33

Processing of personal data

In relation to the processing of personal data present in the evidence subject to exchange through the OOTS and occurring in the components of the OOTS that they own pursuant to Article 25 of this Regulation, the respective competent authorities of Member States, in their capacities as evidence requester or evidence provider, shall act as controllers as defined in Article 4, point 7, of Regulation (EU) 2016/679 and as further specified in Articles 34 and 35 of this Regulation.

Article 34

Responsibilities of evidence requester as data controller

1. For each evidence exchange through the OOTS, the relevant evidence requester or intermediary platform, where applicable, shall be solely responsible for the completeness and lawfulness of the evidence request. The evidence requester shall ensure, in particular, that the evidence is required for the particular procedure for which it is requested by a user.

2. Once the evidence exchanged through the OOTS becomes available to the evidence requester or intermediary platform, where applicable, either following the user's choice to proceed with the exchange of evidence in accordance with Article 14(3), point (f), of Regulation (EU) 2018/1724, or in the case of the procedures referred to in Article 14(5) of Regulation (EU) 2018/1724, the evidence requester or intermediary platform, where applicable, shall ensure the same level of protection of personal data in accordance with Regulation (EU) 2016/679 as in a situation where the user submits or uploads the evidence without having recourse to the OOTS.

Article 35

Responsibilities of evidence provider as data controller

1. Without prejudice to their obligations set out in Regulation (EU) 2016/679, for each evidence exchange through the OOTS, the relevant evidence provider or intermediary platform, where applicable, shall be solely responsible for verifying:

(a) that the requested evidence it holds can be matched to the user in accordance with Article 16;

(b) that the user is entitled to use the requested evidence.

2. When an intermediary platform provides the preview space in accordance with Article 15(1), point (b)(ii), of this Regulation it shall be considered as a processor acting on behalf of the evidence provider according to Article 4(8) of Regulation (EU) 2016/679.

Article 36

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*.

It shall apply from 12 December 2023.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels, 5 August 2022.

For the Commission
The President
Ursula VON DER LEYEN