Formal comments of the EDPS on the draft Commission Implementing Regulation on the technical and operational specifications of the technical system for the cross-border 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

1. Introduction and background

- The draft Commission Implementing Regulation on the technical and operational specifications of the technical system for the cross-border exchange of evidence and application of the "once-only" principle in accordance with Regulation (EU) 2018/1724[1] of the European Parliament and of the Council ('the draft Implementing Regulation') establishes a technical system for the exchange of evidence as required for online procedures listed in Annex II to that Regulation and in 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.

- These formal comments are issued pursuant to Article 42(1) Regulation (EU) 2018/1725 ('the EUDPR')[6], following a request for consultation from the European Commission of 31 March 2021.

- A draft Data Protection Impact Assessment accompanying the draft Implementing Regulation (Commission staff working document) was previously submitted to the EDPS on 12 February 2021 for informal comments. An updated version of the draft Data Protection Impact Assessment was submitted by the European Commission to the EDPS on 26 March 2021. The comments below are limited to the provisions of the Proposal that are relevant from a data protection perspective.

[1] 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 (OJ L 295, 21.11.2018, p. 1). In August 2017, the EDPS issued Opinion 8/2017 in relation to the Commission proposal establishing a single digital gateway and the 'once-only' principle, https://edps.europa.eu/sites/default/files/publication/17-08-01_sdg_opinion_en_0.pdf.
[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).
[6] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).

- These formal comments do not preclude any future additional comments by the EDPS, in particular if further issues are identified or new information becomes available. Furthermore, these formal comments are without prejudice to any future action that may be taken by the EDPS in the exercise of his powers pursuant to Article 58 of Regulation (EU) 2018/1725.

2. Main characteristics of the Once-Only Technical System ("OOTS")

- Article 14(1) of Regulation (EU) 2018/1724 provides that the Commission, in cooperation with the Member States, will establish **a technical system for the automated exchange of evidence** between competent authorities in different Member States.

- The OOTS seeks to enable automated cross-border exchange of evidence among competent authorities at the **explicit request** of citizens or businesses in accordance with the "once-only" principle[7]. The idea is that citizens and businesses should not have to supply the same data to public authorities more than once, and that it should also be possible to use those data at the request of the user for the purposes of completing cross-border online procedures involving cross-border users[8]. Regulation (EU) 2018/1724 also provides that users shall as a rule have the **ability to preview** the evidence to be used by the requesting competent authority and to choose whether or not to proceed with the exchange of evidence[9]. The **procedures for which evidence can be exchanged through OOTS are defined** in Article 14(1) and Annex II of Regulation (EU) 2018/1724.

- According to the draft Commission Implementing Regulation, the OOTS will consist of **several components**, outlined in Article 2. One of the aims of the draft Implementing Regulation is to lay down clear rules on system ownership and the corresponding responsibilities flowing therefrom[10].

- The components which are owned and operated by the Member States include:
    - the relevant evidence requesters' **procedure portals and its back-end**, including a preview area;
    - the evidence providers' **data services**[11];

[7] Without the explicit request of the user, competent authorities may not use the technical system unless otherwise provided under Union or national law (Article 14(4) of Regulation (EU) 2018/1724).
[8] See recital (44) of Regulation (EU) 2018/1724.
[9] See Article 14(3)(f) and 14(5) of Regulation (EU) 2018/1724.
[10] Commission Staff Working Document, Data Protection Impact Assessment, Accompanying the document COMMISSION IMPLEMENTING REGULATION (EU) .../... of XXX 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, p. 12-14 (hereafter: the 'Data Protection Impact Assessment')
[11] A "data service" is defined as a technical service through which an evidence provider handles the evidence requests and dispatches evidence (Article 1(10) of the Commission Implementing Regulation).

- any **intermediary platforms**, where relevant[12];
- **eIDAS Nodes** for user authentication and identity matching[13];
- **eDelivery Access Point(s)**; and
- the **integration elements and interfaces** required to connect these national components with each other and with the common services[14].

Recital (2) of the draft Commission Implementing Regulation clarifies that the OOTS should leverage the existing national procedure portals, data services or intermediary platforms, which have been created for national use[15].

- In addition to the components that are owned and operated by the Member States, the OOTS includes a set of so-called "**common services**"[16], which shall be **established by the Commission** in cooperation with the Member States, and of which **the Commission shall be the owner and responsible entity**[17]. The common services consist of:
  - the **data service directory**;
  - the **evidence broker**;
  - the **semantic repository**;
  - the **common user feedback tool** referred to in Article 9[18].

  The common services are necessary to support the exchange of evidence through the OOTS that takes places *directly* between the so-called national eDelivery Access Points[19]. According to the Data Protection Impact Assessment, the common services

[12] Member States can use new or existing data exchange infrastructures (also known as intermediary services) to retrieve the evidences from the respective data sources within a country's borders (accessing national base registries or local databases). (Commission Staff Working Document on assessment of costs of implementation of the once-only technical system for Member States, p. 2.) See also Articles 1(6), 3, 4, 7, 16, 17 of the draft Commission Implementing Regulation.

[13] The eIDAS node should be used as the cross-border authentication system, implemented under the eIDAS Regulation. See also Commission Staff Working Document on assessment of costs of implementation of the once-only technical system for Member States, p. 2.

[14] Data Protection Impact Assessment, p. 12. See also the Commission Staff Working Document on assessment of costs of implementation of the once-only technical system for Member States Accompanying the document Commission Implementing Regulation (EU) .../... of XXX 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, p. 2-4 (hereafter "Commission Staff Working Document on assessment of costs of implementation of the once-only technical system for Member States").

[15] See also recital (13) of the draft Commission Implementing Regulation.

[16] Data Protection Impact Assessment, p. 13-14.

[17] See Article 4 and Article 22(1) of the draft Commission Implementing Regulation

[18] Article 4 of the draft Commission Implementing Regulation. Each service is further defined and regulated in Article 1 and Articles 5-9 of the draft Commission Implementing Regulation.

[19] Data Protection Impact Assessment, p. 14. For example, "*[t]he evidence broker helps evidence requesters to determine which evidence type from another Member States is equivalent to the evidence it requires for the purposes of a national procedure [...]. This service is based on the data service directory, which contains a list of evidence providers and the evidence they provide. The data service directory also enables evidence requesters to identify the*

do not receive, transmit, have access to or process in any other way the OOTS users' personal data, e.g. the evidence requests or evidences exchanged through the OOTS[20].

3. Roles and responsibilities

- The EDPS welcomes that the draft Implementing Regulation specifies the respective roles and responsibilities of the Member States as evidence requesters and of the evidence providers, as well as those of the Commission, respectively under Chapter III, IV, V and VI.

3.1 The responsibilities and roles of the Member States

- Concerning Article 27 ("Processing of personal data"), the EDPS considers that the draft Implementing Regulation, taking into account the responsibilities of Member States as defined in Chapters II-IV, correctly specifies that "*[i]n relation to the processing of personal data occurring* ***in the components of the OOTS that they own*** *pursuant to Article 27, Member States shall act as* ***controllers*** *as defined in Article 4, point 7, of Regulation (EU) 2016/679 of the European Parliament and of the Council.*"

- The EDPS notes that the Data Protection Impact Assessment further states that the Member States act as *separate* controllers as defined Article 4(7) of Regulation (EU) 2016/679[21]. In this regard, the EDPS notes that **Member States are indeed separate controllers for their respective national systems** and pursue their own (separate) purposes in relation to each evidence request and that each Member State alone and independently of each other on the organisation of their respective national systems[22] in compliance with the national law implementing one of the Directives falling under the scope of the Single Gateway for the cross-border exchange of evidence.

- While Article 19 of the draft Commission Implementing Regulation makes clear that Member States will continue to play an important role in the governance of the OOTS, the EDPS does not consider that this by itself leads to the qualification of joint controllership, insofar as each Member State remains capable of independently determining the purposes and essential means for its own processing of personal data (see also section 3.2 below).

---

level of assurance required by different evidence providers and types of evidence for user authentication and any additional attributes necessary beyond the eIDAS dataset. The semantic repository contains the semantic specifications required to ensure the mutual understanding and cross-lingual interpretation for evidence providers, evidence requesters and the user, when exchanging evidence through the OOTS" (*Id.*).

[20] *Id.*

[21] *Ibid*, p.13.

[22] *Id.*

3.2 The responsibilities and role of the Commission

- As regards the role of the Commission, the draft Implementing Regulation does not assign the role of controller or processor, but rather refers to the Commission as the "owner" of the common services and defines a number of responsibilities. In particular the Commission shall be responsible for:

  > *(a) the development, availability, monitoring, updating, maintenance and hosting of the common services;*
  >
  > *(b) ensuring the security of the common services by preventing any unauthorised access, entry of data and consultation modification or deletion of data, and by detecting any security breaches*"[23].

  The draft Implementing Regulation also assigns the Commission the responsibility of establishing the common services in cooperation with the Member States, who are the intended users of the common services[24]. The Commission must also cooperate with the Member States in developing a high-level architecture to ensure interoperability, which shall be composed of detailed exchange protocols, technical specifications, standards and ancillary services[25].

- As regards the **governance** of the OOTS as a whole (i.e. all components), the draft Implementing Regulation provides that 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, including the implementation of the high-level architecture of the OOTS referred in Article 4(2);*

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

  (c) determine an indicative schedule for regular updates and adaptations of the technical and operational specifications;

  (d) determine criteria for conformity testing to ensure the correct implementation of the technical and operational specifications and the correct functioning of the OOTS;

  (e) adopt risk management plans to identify risks, assess their potential impact and plan responses with appropriate technical and organisational measures in case of incidents.[26]"

---

[23] Article 21 of the draft Commission Implementing Regulation.
[24] Article 4(1) of the draft Commission Implementing Regulation.
[25] Article 4(2) of the draft Commission Implementing Regulation.
[26] Article 19 of the draft Commission Implementing Regulation. See also recital (18) "*Considering that the establishment of the OOTS is a shared responsibility between the Commission and the Member States, the gateway coordination group should play a central role in the governance of the system. In view of the technical nature of its work and to ensure that protocols and specifications can be implemented with ease in existing national systems, the work of the gateway coordination group should be supported and prepared by experts coming together in thematic work package meetings. To ensure a quick reaction to any possible incidents and downtimes which may impact the functioning of the OOTS, the Commission and the Member States should establish a network of technical support*

- In addition, both the Commission and Member States shall designate **contact points for technical support** to ensure a coordinated development, operation and maintenance of the relevant components of the OOTS for which they are responsible pursuant to Chapter VI[27].

- As indicated above, the Data Protection Impact Assessment states that components operated by the Commission (i.e. the common services) enable the exchange of evidence *directly* between the so-called national eDelivery Access Points of the Member States[28]. These components are said not to receive, transmit, have access to or process in any other way the OOTS users' personal data, e.g. the evidence requests or evidences exchanged through the OOTS[29].

- The EDPS further notes that Article 25(3) of Regulation (EU) 2018/1724 provides that the Commission and competent authorities shall have direct access to the user feedback collected through the tool referred to in paragraph 1 of that Article for the purpose of addressing any problems raised[30]. This user feedback tool is, according to the draft Commission implementing decision, one of the "common services" owned by the Commission. Moreover, the EDPS also notes that Article 2 of Regulation 2018/1724 provides that the Commission shall manage a common user interface that is integrated into "Your Europe" portal which will provide links to online procedures, including procedures covered by Annex II of that Regulation[31].

- The EDPS does not see an immediate ground to disagree with the Commission's assessment that it should generally not be considered as a controller in relation to the exchange of personal data that takes place between the Member States through the OOTS. While the draft Implementing Regulation clearly provides for a role in the further design and operation of the OOTS, this role consists primarily in the development, issuance and operation of technical components to facilitate and support direct exchanges of personal data between the Member States, without

---

contact points and provide them with the powers and sufficient human and financial resources to enable them to carry out their tasks."

[27] Article 20 of the draft Commission Implementing Regulation.

[28] Data Protection Impact Assessment, p. 14. For example, "*[t]he evidence broker helps evidence requesters to determine which evidence type from another Member States is equivalent to the evidence it requires for the purposes of a national procedure [...]. This service is based on the data service directory, which contains a list of evidence providers and the evidence they provide. The data service directory also enables evidence requesters to identify the level of assurance required by different evidence providers and types of evidence for user authentication and any additional attributes necessary beyond the eIDAS dataset. The semantic repository contains the semantic specifications required to ensure the mutual understanding and cross-lingual interpretation for evidence providers, evidence requesters and the user, when exchanging evidence through the OOTS"* (*Id.*).

[29] *Id.*

[30] Article 25(1) of Regulation (EU) 2018/1724 requires that the feedback tool shall enable users to signal problems anonymously.

[31] See also Article 21 of Regulation (EU) 2018/1724. Article 24 of Regulation (EU) 2018/1724 requires competent authorities and the Commission to ensure that statistics are collected in relation to users' visits on the gateway and on the webpages to which the gateway links in a way that guarantees anonymity of the users, in order to improve the functionality of the gateway.

determining the "essential means" of the processing[32]. As the nature of these components is clearly delineated by Regulation (EU) 2018/1724 and the draft Implementing Regulation, the EDPS considers that the tasks and responsibilities assigned to the Commission in principle would not allow it to exercise a determinative influence over the purposes and (essential) means of the processing.

- In order to ensure that the role of the Commission remains limited to that of a mere issuer of "technical specifications for the OOTS"[33], operated under the (exclusive) control of the Member States, the EDPS recommends reflecting the limited role of the Commission in the governance structure of the OOTS more clearly (e.g., by clarifying that the activities mentioned in Article 19 shall be performed by the Member States, with support of the Commission)[34]. As clarified by the EDPB in its Guidelines on the concepts of controller and processor: "*Where* ***the controller has been specifically identified by law*** *this will be determinative for establishing* ***who is acting as controller****. This presupposes that* ***the legislator has designated as controller the entity that has a genuine ability to exercise control.***[35]" Therefore, if the further design and operation of the OOTS is to remain under the (exclusive) control of the Member States, the supporting role of the Commission should be delineated more clearly, as well as the procedure that will enable the Member States as controllers to take decisions as to the further design and operation of the OOTS and remain capable of independently determining the purposes and essential means of their own processing activities.

[32] Examples of essential means are the type of personal data which are processed ("which data shall be processed?"), the duration of the processing ("for how long shall they be processed?"), the categories of recipients ("who shall have access to them?") and the categories of data subjects ("whose personal data are being processed?") (See also European Data Protection Board, Guidelines 07/2020 on the concepts of controller and processor in the GDPR Version 1.0, 2 September 2020, paragraph 38, https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf.) See also EDPS, EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725, 7 November 2019, p. 9 and p. 16-17, https://edps.europa.eu/sites/edp/files/publication/19-11-07_edps_guidelines_on_controller_processor_and_jc_reg_2018_1725_en.pdf.

[33] Data Protection Impact Assessment, p. 13.

[34] Compare e.g. with the role of the Commission role of the European Commission within the eHealth Digital Service Infrastructure (eHDSI), even though the Commission is involved in some of the procedures regarding the development of technical and organisational solutions, as well as the systems' security elements, its role as defined in Article 6 of that draft Implementing Decision is clearly articulated as one of technical support in relation to the tasks and responsibilities assigned to the eHealth network. For more information see EDPB-EDPS Joint Opinion 1/2019 on the processing of patients' data and the role of the European Commission within the eHealth Digital Service Infrastructure (eHDSI), in particular at paragraphs 14-18, available at https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-12019-processing.

[35] European Data Protection Board, Guidelines 07/2020 on the concepts of controller and processor in the GDPR Version 1.0, 2 September 2020, paragraph 21, available at: https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf.

4. Additional comments

- The EDPS welcomes the specification of the parameters that shall be contained in the transmission of **the evidence request** from the evidence requester (i.e. the competent authority responsible for one or more of the administrative procedures to be facilitated by the single digital gateway) to the evidence provider (i.e. the competent authority that lawfully issues the evidence needed for the administrative procedure at hand)[36]. These requirements are indeed helpful having regard to compliance with the data protection principle of data minimisation and accuracy pursuant to, respectively, Article 5(1)(c) and 5(1)(d) of Regulation (EU) 2016/679 (hence, 'the GDPR')[37]. To enhance legal certainty, the EDPS recommends further clarifying the draft Implementing Regulation the meaning of the term "**additional attributes**" under Article 14(1)(g), in line with the clarifications provided by the Data Protection Impact Assessment[38].

- As a further safeguard on data quality, the EDPS also welcomes the provisions under Article 15, allowing the user of the technical system the possibility to **preview evidence**, as well as in particular to "*permanently delete the evidence and any cached data from the preview space in case a user decides not to use the evidence for the procedure or when the user leaves the preview space or the procedure portal not explicitly approving the use of the evidence*" (Article 15(1)(c)).

- Article 10 ("Explanation to the users") provides that the evidence requesters shall ensure that their procedure portals contain an explanation about the OOTS and its features, including, in particular, the information that (a) users have the option to preview the evidence and decide whether or not to use it for the procedure; and (b) if the user decides not to use it for the procedure, the previewed evidence will be deleted automatically from the separate preview space referred to in Article 15. The EDPS recommends clarifying that the duty to provide explanation set out in this Article shall be without prejudice to the obligation to ensure the provision of **information to data subjects** as required by Regulation (EU) 2016/679.

---

[36] Article 13 [sic] (Evidence request).
[37] 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).
[38] See Data Protection Impact Assessment, p. 5 ("*Where necessary either for identification or for localising the evidence, the evidence provider can require users to provide additional attributes to access certain types of evidence [...]* and p. 8 ("*Some difficulties for the identity and record matching currently exist because there are different national identification numbers, even several numbers for the same person, and some of those numbers may change over time as well as people's names. This is a general problem, not limited to the OOTS. The OOTS will be designed to work with any new solutions developed and agreed throughout the EU. Where necessary, the evidence providers will be able to require users to use additional attributes to access certain types of evidence. In accordance with the draft Implementing Regulation, those attributes will also be notified in the data service directory. In this case, the evidence requester will have to require the user to input the relevant additional attributes beyond the eIDAS dataset for the purpose of the evidence exchange.*").

- As far as **security** is concerned, the EDPS welcomes that the draft Implementing Regulation also addresses security aspects among the responsibilities of the Commission[39] and of Member States[40]. Both Regulation (EU) 2016/679 and Regulation (EU) 2018/1725 impose a duty to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk[41]. In this regard, the EDPS considers that a **logging and auditing** process may be particularly useful to consider when determining the relevant technical and organisational measures to ensure a level of security appropriate to the risk. This process could consist in a standalone solution managed locally both by the Commission and by the Member States. An integrated approach that centralises the log analysis within the Commission responsibility is also foreseeable. This solution could contribute to reinforce the resilience of processing systems and services as provided both in Article 32(1)(b) of Regulation (EU) 2016/679 and in Article 33(1)(b) of Regulation (EU) 2018/1725.

- While specific information to be logged need to be defined within the information security risk management process, personal data included therein shall be limited to the minimum. Logs could include identifications and affiliations of the user who is operating on the system, date and time of operations, the type of actions performed in the system, and any other information that is necessary to reach the intended purpose. Integrity and availability of the logs should be assured through adequate security measures, while an appropriate retention period should be defined in relation to the purpose[42].

Brussels, 6 May 2021

Wojciech Rafał WIEWIÓROWSKI
(e-signed)

---

[39] Article 21 ("Responsibilities of the Commission"):
"*The Commission shall be shall be the owner of the common services and responsible for the following: [...] (b) ensuring the security of the common services by preventing any unauthorised access, entry of data and consultation modification or deletion of data, and by detecting any security breaches*".

[40] Article 23 ("Responsibilities of the Member States")
"*With respect to the respective national components of the OOTS referred to in Article 2(2), points (a) to (e) and (g), each Member State shall be considered as their owner and responsible for the following: [...] (b) ensuring the security of those components by preventing any unauthorised access, entry of data and consultation, modification or deletion of data and by detecting any security breaches*".

[41] See also EDPS, Guidance on Security Measures for Personal Data Processing, 21 March 2016, https://edps.europa.eu/sites/edp/files/publication/16-03-21_guidance_isrm_en.pdf and EDPS, Guidelines on the protection of personal data in IT governance and IT management of EU institutions, 23 March 2018, https://edps.europa.eu/sites/edp/files/publication/it_governance_management_en.pdf. See also Guidelines on personal data and electronic communications in the EU institutions, available at https://edps.europa.eu/sites/default/files/publication/15-12-16_ecommunications_en.pdf.

[42] For an overview of logging practices and retention periods in the context of the SIS II Decision and Regulation see SIS II Supervision Coordination Group, "Report on logging to the SIS II at national level", available at https://edps.europa.eu/sites/edp/files/publication/18-06-12_sis_report_national_level_en.pdf. See also Article 29 Data Protection Working Party, "Opinion on Commission proposals on establishing a framework for interoperability between EU information systems in the field of borders and visa as well as police and judicial cooperation, asylum and migration", 11 April 2018, WP266, p. 19.