EUROPEAN
COMMISSION

Brussels, XXX
[…](2021) XXX draft

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

INTRODUCTION AND BACKGROUND

On 2 October 2018, the Commission adopted the Single digital gateway Regulation (the "SDGR") which lays down rules *inter alia*, on the establishment of the technical system for the cross-border automated exchange of evidence and implementation of the 'once-only' principle (OOTS) in connection with the procedures listed in Annex II to the Regulation and the procedures provided for in Directives 2005/36/EC, 2006/123/EC/2014/24/EU and 2014/25/EU[1].

Article 14(1) of the SDGR provides that the Commission, in cooperation with the Member States, establishes a technical system for the automated exchange of evidence between competent authorities in different Member States.

Article 14(9) of the SDGR provides that by 12 June 2021, the Commission must adopt an implementing regulation (the "Implementing Act") to set out the technical and operational specifications of the OOTS.

The fundamental questions of the compatibility of the SDGR and the 'once-only' technical system with the data protection rules were assessed in an Opinion issued by the European Data Protection Supervisor (EDPS) in August 2017 (the "Opinion") in relation to the Commission Proposal of the SDGR[2].

The EDPS, in its Opinion, provided specific recommendations as regards the requirements the technical system should meet to ensure compliance with the personal data protection requirements and suggested in particular to clarify:

- the legal basis for the exchange of evidence;
- the notion of explicit request;
- the notion and consequences of the preview;
- the definition of evidence and range of online procedures covered.

All these requirements have been reflected in the provisions of Article 14 of the SDGR and/or in its recitals.

Based on these provisions, the draft Implementing Act describes in more detail how the Commission and the Member States will establish and operate the OOTS and how users will interact with it. The aim of this Impact Assessment is to:

- assess the compliance of the OOTS as foreseen in the Implementing Regulation with the data protection principles;
- identify the data protection risks and possible mitigation measures, also by suggesting the appropriate governance of the system in this regard.

---

[1] Regulation (EU) 2018/1724 of the European Parliament and of the Council 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.

[2] Opinion 8/2017.

- clarify the roles and responsibilities of the actors requesting, receiving and processing evidence to ensure that the rights and freedoms of each data subject are duly protected.

DATA PROTECTION PRINCIPLES AND THE WAY THE OOTS WILL COMPLY WITH THEM

The regulatory framework agreed between the co-Legislators in the SDGR provides the specific requirements in relation to the OOTS to ensure that it fully complies with the relevant data protection requirements.

In particular, Article 14 requires that the OOTS:

- can only be used on an explicit user request;
- ensures the confidentiality and integrity of the evidence;
- enables the user to preview evidence to be used by the requesting competent authority and to choose whether or not to proceed with the exchange of evidence;
- not process evidence beyond what is technically necessary for the exchange of evidence, and then only for the duration necessary for that purpose.

In addition, Article 33 of the SDGR requires that the processing of personal data by competent authorities within the framework of the SDGR must comply with the General Data Protection Regulation (GDPR)[3] and the processing of personal data by the Commission within the framework of the SDGR with Regulation (EU) 2018/1725[4].

Recital 42 to the SDGR also demonstrates this intention of co-legislators to ensure, for the successful implementation of the 'once-only' principle and to enable lawful cross-border exchange of data, that the technical system must be implemented fully in line with the data protection principles including the principle of data minimisation, accuracy, storage limitation, integrity and confidentiality, necessity, proportionality and purpose limitation. Its implementation should also comply fully with the principles of security by design and of privacy by design, and should also respect the fundamental rights of individuals, including those related to fairness and transparency.

After a short description of the OOTS architecture in the following section, the remainder of this document assesses how the OOTS as designed in the draft Implementing Regulation purports to comply with the data protection principles.

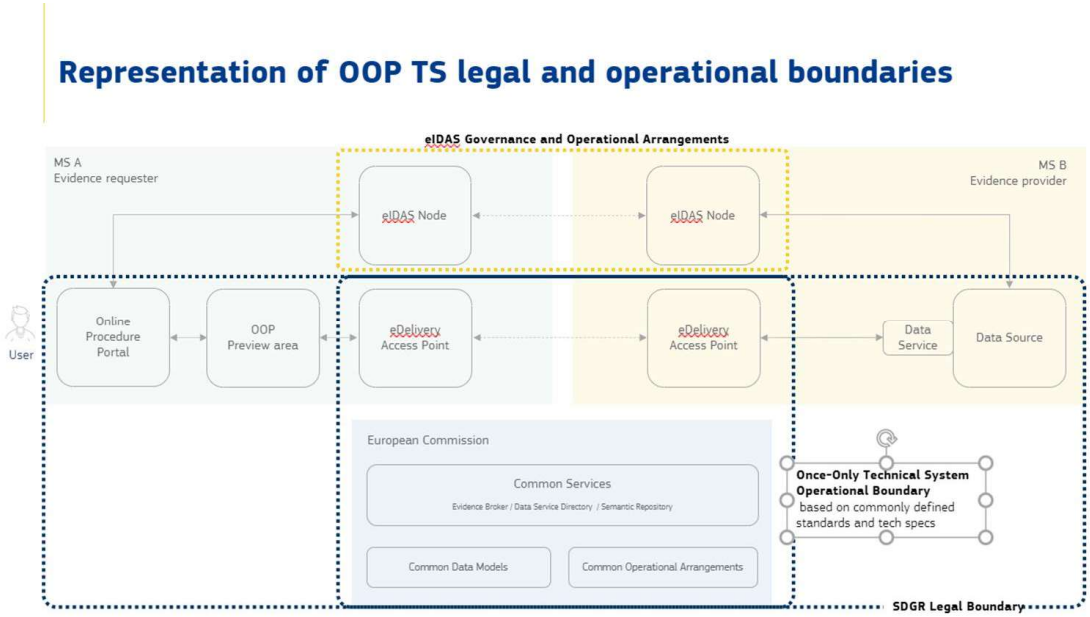
THE EXCHANGE OF EVIDENCE INCLUDING PERSONAL DATA – SCHEMA

The schema presented below shows the architecture of the OOTS as foreseen by the draft Implementing Regulation. The main architectural components managed by Member State A (MS A), who is responsible for a procedure that a user would like to complete, are presented

[3] 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 (OJ L 119, 4.5.2016, p. 1).

[4] 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).

on the left side of the figure (the evidence requester), shaded in green. The right side displays the components managed by Member State B (MS B), the evidence provider, shaded in yellow. The services developed by the Commission in cooperation with the Member States are shown in the centre of the figure (Evidence Broker, Data Service Directory, Semantic Repository, together referred to as the "Common Services"), shaded in blue. They are crucial to enable a user to request the right evidence from evidence providers participating in the OOTS.



"LAWFULNESS" OF PROCESSING - THE LEGAL BASIS OF THE AUTOMATED EXCHANGE OF EVIDENCE THROUGH THE TECHNICAL SYSTEM AND THE EXPLICIT REQUEST

Legal basis

Article 6 of the GDPR requires that personal data shall only be processed if at least one of six legal grounds listed in that Article applies. This requirement is related to the broader principle of 'lawfulness' set forth in Article 5(1)(a), which requires that personal data must be processed 'lawfully'.

The EDPS highlighted in its Opinion that "it is important to distinguish the legal basis of the *exchange of evidence itself* on the one hand and the legal basis for *exchanging the evidence via the technical system* specified in Article [14]" (emphasis added). On this latter point, the EDPS recommended clarifying in a recital that "the legal basis for the use of the technical system specified in Article [14] for the exchange of evidence is performance of a task in the public interest under Article 6(1)(e) of the GDPR".

On the same subject, the EDPS stated that "that any exchange of evidence under Article [14](1) must have an appropriate legal basis elsewhere such as in the four directives listed in Article [14](1) or under applicable EU or national law".

Therefore, in accordance with EDPS Opinion, one needs to distinguish the legal bases for the competent authorities:

a) To request evidence for the purpose of a given procedure;

b) To provide evidence;

c) To use the technical system.

For (a) and (b) national or Union law provides which evidence can be required from a user for which procedures and in which situations and on which basis the evidence held by a competent authority can be submitted to another competent authority or provided to a user (e.g. user request, user consent or performance of a task in the public interest). Recital 45 of the SDGR echoes the EDPS Opinion and recalls that any cross-border exchange of evidence should have an appropriate legal basis such as Directive 2005/36/EC, 2006/123/EC, 2014/24/EU or 2014/25/EU or, for the procedures listed in Annex II, other applicable Union or national law.

Conversely, Art. 14 SDGR provides the legal basis and the scope for the use of the OOTS (point (c)):

- On its basis *evidence requesters* have to enable users to request that the required evidence be transmitted through the OOTS, provided that the evidence is covered by its scope.
- Art. 14 SDGR empowers and obliges *evidence providers* to make the evidence available to the evidence requester if they receive an evidence request through the OOTS. The request can only relate to the evidence types listed in the data service directory foreseen by the draft Implementing Regulation, based on the scope of Art. 14.

The draft Implementing Regulation provides that Member States shall ensure that only evidence providers and evidence requesters, defined as competent authorities that lawfully issue evidence or are responsible for one or more of the procedures falling within the scope of Art. 14, are connected to the OOTS and use its Common Services (Art. 4(3)). It is thus the responsibility of each Member State to ensure that its national components of the OOTS function as a secure closed system.

Moreover, as the EDPS underlined throughout its Opinion, the fact that SDGR is designed in such a way that individuals remain in control of their personal data, notably by requiring an explicit request of the user to initiate the exchange, is in itself a guarantee for a high level of data protection. If the user, when entering the evidence requester's procedural environment or at any later moment in time, has any doubts as to the evidence requester's right to ask for the evidence for the given procedure, s/he remains free to withhold his/her explicit request. In this respect, the OOTS is exactly comparable to the "brick-and-mortar" world where it is also the user's choice to hand over a certain document to a competent authority or not. Moreover, like in the "brick-and-mortar" world, the evidence requesters are bound by the GDPR and obliged to process the evidence exchanged through the OOTS according to its principles.

The draft Implementing Regulation provides that the evidence request, initiated by the user and transmitted to the evidence provider, contains, among other parameters, the name of the competent authority responsible for a procedure and identification of the procedure for which the evidence is required. However, in view of the safeguards listed below, there is no need for **evidence providers** to verify that the evidence requester has a right to request the evidence referred to in the evidence request under the applicable national or regional law:

- The user is at the centre of the system and always remains n control over his/her personal data, as explained above.

- The OOTS is designed as a closed system with a clear distribution of responsibilities (see also the Section on "Division of responsibilities" below). In the example pictured on page 3, only Member State A, where the evidence requester is located, is responsible for and capable of ensuring that the evidence requester connected to the OOTS qualifies as a competent authority within the scope of Art. 14. The evidence requester is also responsible for verifying the identity of the user using secure authentication (eIDAS) and passing the information thus collected on to the evidence provider.

- On the other hand, the evidence provider is ultimately responsible for identity matching and for ensuring that the evidence is only exchanged if the identity attributes sent in the evidence request can be mapped unambiguously to the identity attributes of the user to whom the evidence relates. 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 (for more detail, please see the Section " Authentication of the user and mapping a user to evidence" below).

Explicit request

According to the SDGR, the use of the OOTS is not obligatory for users and is triggered only at their explicit request. Without the explicit request of the user, competent authorities may not initiate the exchange using the Art. 14 SDGR infrastructure unless otherwise provided under Union or national law.

The EDPS recommended in its Opinion to clarify what makes the request 'explicit' and how specific the request must be. The EDPS also stated that the request can only be considered explicit if it contains a freely given, specific, informed and unambiguous indication of the individual's wishes to have the relevant information exchanged, either by statement or affirmative action.

Recital 44 of the SDGR explains the meaning of "explicit request" exactly mirroring the EDPS recommendation.

The draft Implementing Regulation ensures that any request to exchange evidence through the OOTS expressed by a user is "explicit" in the sense of freely given, specific, informed and unambiguous in the following way:

- Article 10 specifies the information to be given to the user when s/he enters the evidence requester's procedure portal, namely the functioning of the OOTS, the option to preview the evidence and decide whether or not to use it for the procedure and the automatic deletion of evidence that the user decides not to use for the procedure.
- Pursuant to Article 11 of the draft Implementing Regulation, the user is then provided with a selection of evidence(s) relevant to the procedure in question and that can be exchanged through the OOTS.
- Article 13 provides that after pre-selecting a type or types of evidence, the evidence requester shall ensure that the user can make an informed explicit request by displaying the name(s) of the evidence provider(s) and the evidence type(s) or data fields that will be exchanged. Only at the end of this process will the user be able to request the selected evidence (e.g. by clicking on a button).

The user request cannot be equalled with consent under Article 6(1)(a) of the GDPR. As explained above, there must be a legal basis in national or Union law for the evidence requester to request and the evidence provider to provide the relevant evidence. A user who launches an administrative procedure does therefore not, like for example a data subject contemplating a commercial transaction, have a choice to provide the evidence required for a procedure or not; his/her choice is limited to completing the procedure and obtaining the desired outcome by submitting the required evidence, or abandoning the procedure and its outcome.

A user also has a choice as regards to the manner in which s/he provides the evidence:

- By physical displacement (if physical interaction is allowed);
- By obtaining and uploading the required evidence himself;
- By using the OOTS (provided that the evidence is covered by Article 14 SDGR).

The user's explicit request pursuant to Article 14(3)(a) and (4) SDGR relates to this choice: by expressing his/her explicit request, the user only agrees to use the OOTS as a channel for an exchange of evidence that has its legal basis elsewhere.

PREVIEW – USER CONTROL OVER PERSONAL DATA AND DATA ACCURACY AND INTEGRITY

The EDPS stated that offering the possibility for the user to 'preview' the evidence to be exchanged is not only, together with requiring the user's explicit request, a guarantee that the user remains in control of his/her personal data, but also helps to ensure that any evidence exchanged is adequate, relevant, limited to what is necessary in relation to the purposes for which they are processed ('data minimisation') as well as accurate and, where necessary, kept up to date ('data accuracy and integrity'). A user preview, as envisaged by the EDPS, would ensure that only correct data are transferred.

These principles were already enshrined in the SDGR. According its Article 14(3)(f), the preview shall enable the user to make a decision about whether to proceed with the exchange and allow the user to abort the exchange, if he discovers for instance that the information is inaccurate, out-of-date, or goes beyond what is necessary for the procedure in question. Recital 47 of the SDGR states that *"(...) the user should have the possibility to preview the evidence and the right to choose not to proceed with the exchange of evidence in cases where the user, after previewing the evidence to be exchanged discovers that the information is inaccurate, out-of-date, or goes beyond what is necessary for the procedure in question."*

The draft Implementing Regulation takes great care to stipulate the details of preview in such a way that it can fulfil in practice its double role of putting the user in control of his/her personal data and enabling the user to verify that the previewed evidence is adequate, relevant, limited to what is necessary, accurate and up-to-date. This process starts when the user enters the procedural environment of the evidence requester and his/her attention is drawn to the fact that users have the option to preview the evidence and decide whether or not to use it for the procedure; and that the previewed evidence will be deleted automatically if the user decides not to use it for the procedure (Article 10 of the draft Implementing Regulation). This information is important not only to familiarise users with the OOTS, but also to induce them to make active use of the preview possibility without the fear that any personal data could be disseminated against their will.

Article 15 of the draft Implementing Regulation lays down in the detail the features of the preview with a view to optimising its effectiveness as regards data protection. It provides in particular that the preview space must be separate and equipped with technical features that:

- allow only the user to access it and only as long as the user is in the procedure environment and until the user decides whether or not to use the previewed evidence in the procedure;
- do not allow the evidence requester or any third parties to access, view or copy the evidence in the preview space;
- permanently delete the evidence and any cached data 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.

These provisions ensure that, if the user, based on the preview decides that the information is inaccurate or otherwise unsuitable for submission as part of the procedure, s/he can abort the exchange. In such cases, s/he would need to provide the evidence via other means, for instance a scanned copy or other electronic format of the evidence that s/he can obtain him/herself.

If the evidence requester considers that the evidence provided through the OOTS is inaccurate or of low quality, it is its responsibility to assess the evidence submitted as part of the relevant procedure, just like it would be the case in the "brick-and-mortar" world where the user hands over a certain document issued by a competent authority in one Member State to a competent authority in another Member State. In case of doubt, the evidence requester can ask for clarifications through the Internal Market Information System (IMI). If there is a systemic problem with the quality of evidence from a specific authority, this problem can be raised in the SDG coordination group.

In addition, as emphasised by the EDPS in its Opinion, while the preview mechanism helps ensure compliance with data quality, it follows from the generally applicable data protection rules that the competent authorities should still put in place effective procedures to ensure that personal data is updated where necessary and that inaccurate or outdated data are no longer processed. This is a general obligation independent from the use of the OOTS.

The preview is an important guarantee offered to the user by the OOTS. The location of the preview space in the procedural environment of the evidence requester as foreseen by the draft Implementing Regulation does not affect its value for user control nor compromise the security of the user's personal data, even though the preview requires the prior transmission of the evidence from the evidence provider to the evidence requester. First, Article 1(3) GDPR establishes the principle of free movement of personal data within the Union. The cross-border exchange occurs within the Union and all actors involved are bound by the GDPR. Moreover, this intra-EU exchange of evidence is the very purpose of the OOTS foreseen by the SDGR and, as recalled, accompanied by data protection safeguards. Second, as described in more detail above, Article 15 of the draft Implementing Regulation foresees a number of additional safeguards to ensure that the previewed evidence can only be accessed by the user and is not stored or used by the evidence requester, or any other person, when the user chooses not to proceed with the evidences exchange. This way of proceeding is exactly the same as in the "brick-and-mortar" world where users only submit evidence that they themselves have obtained from the relevant authorities.

DATA CONFIDENTIALITY

The principle of data confidentiality implies that the data should be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

Authentication of the user and mapping a user to evidence

The electronic identification of a user is primordial for the security of the OOTS as it enables the evidence provider to ascertain without doubt that a user requesting the evidence is entitled to receive such evidence.

To that effect, the draft Implementing Regulation builds on the security mechanisms offered by Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market, which offers reliable guarantees in terms of security.

To this end, Article 3(1) of the draft Implementing Regulation provides that evidence requesters must be connected (directly or indirectly) to an eIDAS node to perform the user authentication when using the OOTS. eIDAS nodes implement the technical specifications developed in line with Regulation (EU) No 910/2014, enabling the communication with other nodes of the eIDAS network for the purpose of cross-border authentication. The draft Implementing Regulation also provides that it is for the evidence providers to determine the level of assurance of electronic identification notified by Member States in accordance with Regulation (EU) 910/2014, required for the exchange through the OOTS of different types of evidence that they issue. This information will be recorded in the data service directory.

On that basis, the evidence requester verifies the identity of users by obliging them to authenticate using electronic identification means notified by the Member States in accordance with the eIDAS Regulation, meeting the assurance level substantial or high requested by the evidence provider, as recorded in the data service directory.

The evidence request, which will be transmitted through the technical system to the evidence provider will contain the personal identification data received when authenticating the user and the level of assurance of the eID means used for the authentication.

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.

The draft Implementing Regulation (Article 17) states that the ultimate responsibility for record matching lies with the evidence provider. The evidence is only exchanged if the identity attributes sent in the evidence request can be mapped unambiguously to the identity attributes

of the user to whom the evidence relates. Where the identity record matching does not result in an unambiguous match, the requested evidence will not be exchanged.

In short, the draft Implementing Regulation

- Builds on proven and pre-existing building blocks for secure user authentication (eIDAS);
- Empowers the evidence providers to require a higher level of assurance for authentication than would be required by the evidence requester if this is considered necessary;
- Allows for additional attributes to be exchanged if this is required for certain types of evidence; and
- Does not allow for evidences to be exchanged through the OOTS unless the evidence request can be mapped unambiguously to the identify attributes of the user to whom requested evidence relates.

These measures taken together ensure a high level of security in authenticating and mapping users to evidence.

Security and confidentiality during the transmission of data

Like for user authentication, the draft Implementing Regulation builds the OOTS on proven and pre-existing building blocks for secure data transmission between Member States/competent authorities, namely eDelivery Access Points. eDelivery Access Points are building blocks developed under the Connecting Europe Facility Programme that provide technical specifications and standards, installable software and ancillary services which allow to create a network of nodes for secure digital data exchange. The delivery services provided through eDelivery Access Points comply with the requirements for qualified electronic registered delivery services, laid down in Article 44 of Regulation (EU) 910/2014.

Pursuant to Article 3(2), the Member States will need to install, configure and integrate the eDelivery Access Points in their IT systems. These Access Points are thus one of the national components of the OOTS for which the Member States are responsible according to Article 23 of the draft Implementing Regulation, in particular for ensuring their security by preventing any unauthorised person from having access to them, preventing the entry of data and any consultation, modification or deletion of data by unauthorised persons and detecting any security breaches.

The draft Implementing Regulation also establishes a network of single points of contact in the Member States (Article 20) that will handle any possible downtimes of the eDelivery Access Points or possible security breaches, as well as investigate and fix incidents.

DATA MINIMISATION AND PURPOSE LIMITATION

Principles of purpose limitation and data minimisation

Data protection by default requires ensuring that data processing activities are conducted only if they are necessary to achieve a specific goal. It links to the GDPR's principles of data minimisation and purpose limitation.

The principle of **purpose limitation** is a key principle of data protection requiring that personal data must be 'collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes'. To implement this principle (subject to some exceptions), Article 6(4) of the GDPR requires that the different purposes for which personal data are to be processed should be assessed against the purpose for which the data were initially collected in order to ensure compatibility. Article 6(4) lists the following factors, which must, in particular, be taken into account during the compatibility assessment:

- link between the initial and further purposes;
- context of collection, including the relationship between the individual and the controller;
- nature of the data (including whether special categories of data are processed);
- the possible consequences for the individuals, and
- safeguards (including encryption or pseudonymisation).

According to the principle of **data minimisation**, the processing of personal data should be :

- adequate – sufficient to properly fulfil the purpose;
- relevant – has a rational link to that purpose; and
- limited to what is necessary – not more than what is needed for that purpose.

Data which can be exchanged through the OOTS

Article 14(1) SDGR limits the number of procedures for which evidence can be exchanged through the OOTS.

According to Article 3(5) of the SDGR, evidence means any document or data, including text or sound, visual or audio-visual recording, irrespective of the medium used, required by a competent authority to prove facts or compliance with procedural requirements (…).

While this definition also covers evidence in both paper and electronic format, Article 14(2) limits the type of evidence that can be exchanged through the OOTS to evidence lawfully issued by a competent authority and in an electronic format allowing automated exchange.

The evidence qualifying for an exchange through the OOTS has thus to fulfil three requirements:

- Has to be legally issued by the competent authority;
- Has to be in electronic format;
- Can be exchanged in an automated fashion.

Application of the principles of purpose limitation and data minimisation to the data exchanged

In the OOTS, the **purpose limitation principle** is guaranteed as the data which can be requested are collected for specific, explicit and legitimate purposes, *i.e.* for completing the specific procedure requested by the user and covered by Article 14 SDGR.

The **data minimisation principle** is guaranteed in three steps:

- With the help of the data service directory (lists the evidence providers and the evidences which can be exchanged through the technical system, see Article 5 of the draft Implementing Regulation) and the evidence broker (allows the automated matching between evidences from different Member States, see Article 6 of the draft Implementing Regulation), the evidence requester will show to the user the evidence or evidences which is/are equivalent to the evidence that is needed for the given procedure;
- On that basis, the user can then select the relevant evidence(s) and express an explicit request;
- Finally, the preview system will enable the user to see which personal data will be accessible to the evidence requester and to agree to it or not;

If the evidence provider can only provide (unstructured) digitalised documents, instead of (structured) data, it is possible that the evidence requester receives more personal data than strictly needed for a given procedure. However, this situation is no different from situations in which such evidence is submitted by the user in the physical world. The SDGR does not harmonise the format in which evidence is provided by the different competent authorities in the Member States. Until all administrations move to a system based on data instead of documents, the once-only system should be able to accommodate both categories of evidence: structured and unstructured (for the definitions of these categories of evidence see the Implementing Regulation), provided that they can be exchanged in an automated fashion.

STORAGE LIMITATION - THE APPROACH TO FILING AND STORAGE OF THE EXCHANGED DATA

Article 14(3)(i) SDGR states that " the technical system shall not process evidence beyond what is technically necessary for the exchange of evidence, and then only for the duration necessary for that purpose".

The duration of processing of evidence through the OOTS is different from the duration of processing of that same evidence by the evidence requester. For the purpose of transmission through the OOTS, the exchange of the evidence request and the evidence should be kept through one session: from the moment the user makes his request, through the transmission of the evidence request, receiving of the request on the side of evidence provider, dispatching of evidence, transfer to the preview phase to a moment when a user submits the application. As explained above, Article 15 provides that the evidence previewed by the user is permanently deleted 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. If a user decides to use the evidence and to follow through with the procedure, the evidence requester should follow national rules and the principles enshrined in the GDPR concerning the storage of evidence (as it is already the case for any other procedure).

SECURITY BY DESIGN

In line with its Article 1(3), the SDGR does not affect measures taken in accordance with Union law to safeguard cybersecurity and to prevent fraud. Those relevant Union and national acts apply also to the OOTS.

In addition, the draft Implementing Regulation lays down clear rules on system ownership and the corresponding responsibilities flowing therefrom. The Common Services are owned and operated by the Commission while the Member States own and operate their respective national systems. These national systems are composed of:

- the relevant evidence requesters' procedure portals;
- the evidence providers' data services; any intermediary platforms, where relevant;
- eIDAS Nodes for user authentication and identity matching;
- eDelivery Access Point(s); and
- the integration elements and interfaces required to connect these national components with each other and with the Common Services.

Pursuant to Articles 22 and 23 of the draft Implementing Regulation, the Commission and the Member States are responsible for the components that they own and operate, in particular for ensuring the security of those components by preventing any unauthorised access, entry of data and consultation, modification or deletion of data and detecting any security breaches.

The draft Implementing Regulation also establishes a network of single points of contact in the Member States (Article 20) that will handle any possible downtimes of the various components or possible security breaches, as well as investigate and fix incidents.

DATA CONTROLLER AND DATA PROCESSOR – DIVISION OF RESPONSIBILITIES

Article 14 of the SDGR lays down the overall purpose and the essential features of the OOTS and provides that the Commission should adopt implementing acts to set out the technical and operational specifications of the OOTS. In doing so, the Commission ensures that the different national components are and remain interoperable and integrate certain trusted and secure building blocks (notably eDelivery Access Points and eIDAS nodes), and that the essential features foreseen by Article 14 of the SDGR are complied with (for instance the preview possibility).

The OOTS will be composed of different components as shown in the picture on page 3. As explained above, the draft Implementing Regulation lays down which system components are established, operated and owned by the Member States respectively (i.e. their respective national systems, listed in the previous section) and which components by the Commission (i.e. the Common Services).

The Member States as owners and controllers of their respective national systems and masters of the procedures in the context of which the evidence is exchanged

According to Article 4(7) of the GDPR, a controller *"determines [alone or jointly with others], the purposes and means of the processing of personal data (...)"*.

Article 26 of the GDPR specifies that the controllership is joint "*where two or more controllers jointly determine the purposes and means of processing*". According to the EDPB guidelines on the concepts of controller and processor in the GDPR, "*assessing the existence of joint controllers requires examining whether the determination of purposes and means that characterize a controller are decided by more than one party. "Jointly" must be interpreted as meaning "together with" or "not alone" (…). The assessment of joint controllership should be carried out on a factual, rather than a formal analysis of the actual influence on the purposes and means of the processing*"[5]. The guidelines go on to state that "*joint participation needs to include the determination of purposes on the one hand and the determination of means on the other hand. If each of these elements are determined by all entities concerned, they should be considered as joint controllers of the processing at issue*"[6]. However "*an entity will be considered as joint controller with the other(s) only in respect of those operations for which it determines, jointly with others, the means and the purposes of the processing. If one of these entities decides alone the purposes and means of operations that precede or are subsequent in the chain of processing, this entity must be considered as the sole controller of this preceding or subsequent operation"*[7].

For the purposes of the OOTS, it is useful to draw a distinction between the purpose and the means of the exchange of evidence:

- While the overall, abstract purpose of the OOTS is laid down in the SDGR, the specific **purpose** of an exchange of evidence, for example the exchange pictured on page 3, is determined by Member State A where the evidence requester is located, because it is Member State A (or one of its sub-entities) that determines which pieces of evidence are required for any given procedure covered by Article 14 of the SDGR. Member B, the evidence provider, has no say in this.

- The **means** of the exchange are determined by Member States A and B, each for their respective national systems, which they own and operate within the boundaries of the SDGR and the draft Implementing Regulation. However, Member States A and B decide alone and independently of each other on the organisation of their respective national systems.

In conclusion, the Member States act thus as (separate) controllers as defined Article 4(7) of the GDPR and are bound by the obligations laid down in that Regulation in relation to their respective national components of the OOTS.

Conversely, the Commission only intervenes as issuer of technical specifications for the OOTS. According to the EDPB guidelines, in the absence of access to the personal data being processed, an actor has to have influence on the purpose of the processing of personal data **and** on the (essential) means of the processing ("*e.g. by adjusting parameters of a service in such*

[5] "Guidelines 07/2020 on the concepts of controller and processor in the GDPR", as available for the public consultation, adopted in September 2020 by the EPDB, p. 17, pt. 48-49.

[6] "Guidelines 07/2020 on the concepts of controller and processor in the GDPR", as available for the public consultation, adopted in September 2020 by the EPDB, p. 17, pt. 50.

[7] Guidelines 07/2020 on the concepts of controller and processor in the GDPR", as available for the public consultation, adopted in September 2020 by the EPDB, p. 18, pt. 55.

a way that it influences whose personal data shall be processed") to qualify as a controller[8]. This is not the case here since the abstract purpose of the processing is determined by the SDGR itself and the concrete purpose of each exchange of evidence by the evidence requester or relevant Member State. Any finding to the contrary would mean that the Commission would be a (joint) controller for example in the myriad of instances in which operators use in their systems the eDelivery and eIDAS specifications and protocols developed by the Commission to process personal data.

The role of the Commission as owner and operator of the common services

The Common Services under the responsibility of the Commission support the exchange of evidence through the OOTS that takes places directly between the national eDelivery Access Points. The 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, especially in situations where there is no agreed evidence type that is harmonised across the EU and that all Member States can provide. 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. The Common Services are indispensable for the functioning of the OOTS, but they 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.

Based on how the OOTS functions and the involvement of the Commission as owner and operator of the Common Services, it can be concluded that the Commission does not act as a data controller or processor within the meaning of Article 4(7) and (8) of the GDPR.

CONCLUSION

The OOTS as designed in the draft Implementing Regulation complies with the relevant provisions of the SDGR and the data protection requirements, while ensuring the user-friendliness of the system which is essential to guarantee the use of the system.

[8] Guidelines 07/2020 on the concepts of controller and processor in the GDPR", as available for the public consultation, adopted in September 2020 by the EPDB, p. 16, pt. 42.