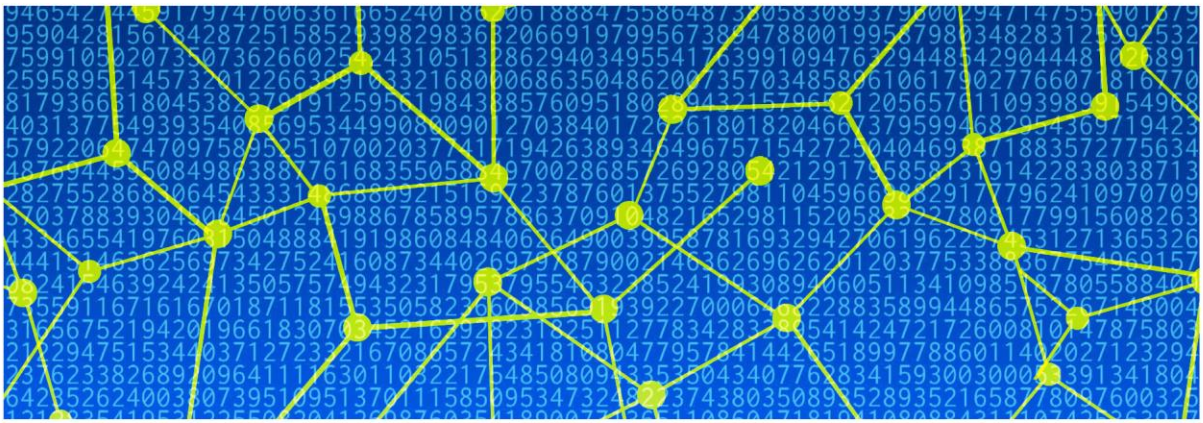

EUROPEAN DATA PROTECTION SUPERVISOR

Opinion 5/2019

on the revision of the EU Regulations on service of documents and taking of evidence in civil or commercial matters

EDPS

13 September 2019

The European Data Protection Supervisor (EDPS) is an independent institution of the EU, responsible under Article 52(2) of Regulation 2018/1725 'With respect to the processing of personal data… for ensuring that the fundamental rights and freedoms of natural persons, and in particular their right to data protection, are respected by Union institutions and bodies', and under Article 52(3)'…for advising Union institutions and bodies and data subjects on all matters concerning the processing of personal data'. Under Article 57(1)(g) of Regulation 2018/1725, the EDPS shall 'advise on his or her own initiative or on request, all Union institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to the processing of personal data'.

He was appointed in December 2014 together with the Assistant Supervisor with the specific remit of being constructive and proactive. The EDPS published in March 2015 a five-year strategy setting out how he intends to implement this remit, and to be accountable for doing so.

This Opinion provides advice on two Commission proposals for the revision of the Regulations on the service of documents and the taking of evidence in civil or commercial matters, in particular with regard to the use of an IT system for their purposes.

Executive Summary

On 31 May 2018, the European Commission issued two proposals for a Regulation of the European parliament and the Council amending Council Regulation (EC) No 1206/2001 of 28 May 2001 on cooperation between the courts of the Member States in the taking of evidence in civil or commercial matters, on the one hand and a Regulation amending Regulation (EC) No 1393/2007 of the European Parliament and of the Council on the service in the Member States of judicial and extrajudicial documents in civil or commercial matters, on the other hand. The proposals mainly aim at improving the smooth functioning of judicial cooperation in these areas, by inter alia providing for transmission of documents and taking of evidence requests through a decentralised IT system.

The EDPS acknowledges that exchanges of personal data are necessary elements of the creation of an area of Freedom, Security and Justice. Therefore he welcomes the overall objectives of the proposals to improve the efficiency of judicial cooperation in civil or commercial matters in relation to the taking of evidence and the service of documents, in particular through digitalisation and the use of IT technology. He shares the view that the proposed legislation could have a real impact on the everyday lives of EU citizens.

This Opinion makes three main recommendations in order to constructively assist the legislators in achieving this very important objective while ensuring compliance with the Charter and the GDPR:

- providing a clear legal basis for the IT system which would be used for the transmission of documents, requests and communications for the purposes of these Regulations. In particular, in case the IT system would entail the involvement of an EU institution, body, agency or office, this legal basis should in principle be provided in an EU legislative act. Also, even in case the processing of personal data would take place in the framework of an existing IT system, the EDPS recommends providing for the use of such system in the legislative act itself. However, the existing system envisaged to be used should itself be duly established on the basis of a legal act adopted at EU level, which is currently not the case of e-CODEX. Should the EU legislator choose the e-CODEX solution, the lack of a legal instrument at EU level establishing and regulating the system should be remedied without delay.

- including in the legislative acts themselves a high level description of the IT system aspects, such as data protection responsibilities or relevant applicable safeguards, to be further defined in implementing acts. In particular, to the extent the Commission or another EU institution, body, agency or office would be implicated in the operation of the new system, the legal act should ideally define its responsibilities as a (joint) controller or a processor.

- conducting an impact assessment on data protection when preparing the implementing acts.

Further detailed recommendations are provided by the EDPS in this Opinion.

The EDPS remains at the disposal of the institutions for further advice during the legislative process and at the implementing phase of the Regulations once adopted.

TABLE OF CONTENTS

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16 thereof,

Having regard to the Charter of Fundamental Rights of the European Union, and in particular Articles 7 and 8 thereof,

Having regard to 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)[1],

Having regard to 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[2], in particular Articles 42(1), 57(1)(g) and 58(3)(c) thereof,

HAS ADOPTED THE FOLLOWING OPINION:

1. Introduction and background

1. On 31 May 2018, the Commission adopted two proposals[3] for a Regulation of the European parliament and the Council that would amend:

   – Council Regulation (EC) No 1206/2001 of 28 May 2001 on cooperation between the courts of the Member States in the **taking of evidence in civil or commercial matters** (hereinafter the "taking of evidence Regulation");

   – Regulation (EC) No 1393/2007 of the European Parliament and of the Council on the **service in the Member States of judicial and extrajudicial documents in civil or commercial matters** (hereinafter the "service of documents Regulation").

2. The taking of evidence Regulation, which has applied since 2004, provides for two ways of taking of evidence between Member States: taking of evidence through the requested court and the direct taking of evidence by the requesting court.

3. The service of documents Regulation, which has applied since 2008, provides for different ways of transmitting documents from one Member State to another, for purposes of service in the latter, through transmitting and receiving agencies or through transmission by consular or diplomatic channels. It also sets uniform legal conditions for serving a document by post directly across borders and provides for a direct service through the competent person of the Member State addressed where permitted under the law of that Member State. It includes certain minimum standards on the protection of the rights of defence. The application of the Regulation "*is not restricted to proceedings before civil tribunals, because its scope covers also 'extrajudicial' documents, the service of which may arise in various out-of-court proceedings (e.g. in succession cases before a public notary, or in family law cases before a public authority), or even in the absence of any underlying judicial proceedings*"[4].

4. The proposals are included in the Commission's 2018 work programme under REFIT initiatives in the area of justice and fundamental rights based on mutual trust[5]. The proposals are accompanied by an impact assessment[6].

5. Both proposals provide for the transmission of documents, requests and communications through a mandatory decentralised IT system composed of national IT systems interconnected by a communication infrastructure enabling the secure and reliable cross-border exchange of information between the national IT systems. They also provide for the application of Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market[7].

6. On 13 February 2019, the European Parliament adopted its legislative resolutions on both proposals at first reading[8], *inter alia* agreeing on the establishment of a decentralised IT system, providing that such system be based on e-CODEX and that the implementation of such system be ensured via delegated acts.

7. On 6 June 2019, a policy debate took place in Council. The presidency concluded that "*the Council confirmed the need to modernise our processes when it comes to judicial cooperation in civil and commercial matters. The presidency noted the preference expressed for a decentralised and secured IT system. It added that ministers could accept mandatory use of the system only with certain conditions, including a longer transition period and with a backend reference system to be provided by the Commission. A list of necessary exceptions will also have to be considered. Finally, the presidency noted that e-CODEX could be the software solution to be used for that purpose. Further work will have to be conducted at technical level"*[9].

8. On 23 April 2019, the Commission has submitted a request for consultation to the European Data Protection Supervisor (hereinafter the "EDPS") in order to assess the conformity of both proposals with the General Data Protection Regulation (hereinafter the "GDPR"). The EDPS welcomes the consultation by the Commission.

2. Recommendations

2.1. Legal basis

9. The EDPS acknowledges that exchanges of personal data are indispensable for the creation of an area of Freedom, Security and Justice. Therefore he welcomes the overall objectives of the proposals to improve the efficiency of judicial cooperation in civil or commercial matters in relation to the taking of evidence and the service of documents, in particular through digitalisation and the use of IT technology. He shares the view that such legislation may have a real impact on the everyday lives of EU citizens.

10. The EDPS recalls that any establishment of a new IT system processing personal data as well as its essential elements require a legal basis[10]. He stresses in particular that **where such IT system entails the involvement of an EU institution, body, agency or office, this legal basis should in principle be provided in an EU legislative act.**

11. Also, even in case the processing of personal data would take place in the framework of an existing IT system, **the EDPS recommends providing for the use of such system in the**

legislative act itself. However, the existing system envisaged to be used should itself be duly established on the basis of a legal act adopted at EU level, which is currently not the case of e-CODEX. Should the EU legislator choose the e-CODEX solution, the lack of a legal instrument at EU level establishing and regulating the system should be remedied without delay.

2.2. Legislative acts

12. **The EDPS recommends including in the legislative acts a high level description of the IT system aspects to be further defined in implementing acts**. These elements, based on an assessment of the risks for the fundamental rights of the individuals, should cover at least data protection responsibilities (i.e. the roles of controller, joint controller, processor, as appropriate) as well as relevant applicable safeguards, including those to ensure the security of the personal data processed. Respect for data protection is not only a legal obligation but also a key element for success of the envisaged system, e.g. ensuring quality of data exchanges.

2.2.1. Principles of data protection by design and by default

13. The explanatory memorandum of both proposals underlines that *"[i]mportant external factors with regard to the protection of personal data in the context of the proposed policy package are: – the General Data Protection Regulation (GDPR), applied as of May 2018, which should increase awareness and prompt action to ensure the security and integrity of databases, and swift reactions to breaches of privacy in the judiciary; (...)"*[11]. As the GDPR is applicable to the processing of personal data for the purposes of judicial cooperation in civil or commercial matters under both Regulations, the EDPS recommends applying its principles already at the stage of setting up the IT system, in particular **the principles of data protection by design and by default** set out in Article 25 of the GDPR.

14. In this regard, **the EDPS welcomes the identification of a high-level architecture of the system in the legislative acts themselves and the obligation of a reliable exchange of information as well as the need to use trust services as defined in 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**[12]. He recalls that the choice of the IT system architecture minimising the impact on data protection should be made based on an assessment of the risks for the individuals whose data are processed, rather than on what architecture minimises possible responsibilities of the Member States or EU institutions. Unless there is a specific need for centrally based functionalities, a decentralised architecture might indeed, in general, avoid single points of failure and support the data minimisation principle.

15. The explanatory memorandum of both proposals underlines that the other important external factor to take into account is the "*persistent threats to cybersecurity in the public sector. Attempted attacks on public IT infrastructure are expected to proliferate and to affect the judiciary in the Member States; their impact may be exacerbated by the growing interconnectedness of IT systems (nationally and at EU level)*"[13]. It is utterly important that the data processed in this IT system are protected against any possible attackers and security incidents. In particular, with regard to **the taking of evidence proposal, the EDPS recommends being more specific on the required appropriate safeguards to ensure**

the security of the videoconference[14]. These safeguards should be further detailed in the implementing act (see section 2.3. below).

2.2.2. Definition of responsibilities

16. The EDPS underlines that the choice of a decentralised architecture automatically entails that the Member States are responsible for the civil or commercial records databases and the processing of personal data within these databases. More specifically, the authorities of the Member States are the controllers of the record databases that they are responsible for. As such, they are responsible for the content of the databases and for the integrity of the information that is exchanged. It is essential to ensure that responsibilities with regard to compliance with data protection rules are clearly defined and allocated.

17. Whereas the proposals aim at establishing a high level architecture for the planned IT system, it does not define governance and high level roles and responsibilities of the Member States and of the Commission (if any). These roles and responsibilities are however essential for assigning the controller role and relevant obligations under the applicable data protection law. To the extent the Commission or another EU institution, body, agency or office would be implicated in the operation of the new system, the legal act should ideally define its responsibilities as a (joint) controller or a processor. **The EDPS therefore strongly recommends defining governance and high level roles and responsibilities of the Member States and of the Commission or any other EU institution, body, agency or office (if any) in the legislative act.** In case there would be a role for the Commission or any other EU institution, body, agency or office in the processing of these data, Regulation No 2018/1725 would be applicable to such processing.

18. In case of joint controllership, obligations of Article 26 of the GDPR or Article 28 of Regulation No 2018/1725 would apply and **the relationship among joint controllers and the content of the mandatory arrangements among them should be defined in the implementing acts.**

2.3. Implementing acts

19. The EDPS notes that only the service of documents proposal foresees the adoption of an implementing act for the establishment of the decentralised IT system[15]. **He therefore recommends providing for such implementing act in both proposals.**

20. Such implementing acts should lay down important elements of the system in more detail. They should also help ensure compliance with data protection requirements by further specifying necessary safeguards to be implemented in the IT system. Consequently**, the EDPS recommends providing in the legislative acts for the implementing act to cover also the new provisions on electronic service[16] and on direct taking of evidence by videoconference[17].**

21. As the impact assessments accompanying the proposals do not contain any in depth analysis of the impact of these proposals on data protection, **the EDPS strongly recommends the Commission to conduct an impact assessment when preparing the implementing acts.** This is without prejudice to obligations of controllers under the GDPR and, as the case may be, Regulation No 2018/1725, to in particular conduct a Data Protection Impact Assessment

as provided for under Article 35 of the GDPR or Article 39 of Regulation No 2018/1725, should the conditions be fulfilled[18].

22. Furthermore, from the explanatory memorandum of both proposals[19], the EDPS understands that the future IT system might be the same for both of them and that its access would be limited to specific users: for the taking of evidence proposal, the number of users would be limited to the courts[20], central authorities and competent authorities within the meaning of the Regulation, as communicated by the Member States while for the service of documents proposal, the number of users would be limited to transmitting and receiving agencies[21] and central bodies designated by the Member States. The EDPS **recommends that safeguards ensuring an access to a limited number of authorised users be specified in the implementing acts.**

23. Finally, the proposals would introduce a new Article 23a to the service of documents Regulation and a new Article 22a to the taking of evidence Regulation according to which Member States shall provide the Commission with the data and other evidence necessary for the monitoring programme that the Commission shall establish by two years after the date of application of the Regulations. The EDPS understands that these monitoring programmes would entail the collection of statistical data[22] and **recommends that the statistical elements to be collected be defined in further detail as far as possible in the implementing acts.**

3. Conclusions

24. The EDPS welcomes the overall objectives of the proposals to improve the efficiency of judicial cooperation, in particular through digitalisation and the use of IT technology, in relation to the taking of evidence and the service of documents in civil or commercial matters. Therefore, this Opinion aims at providing constructive and objective advice to the EU institutions.

25. The EDPS welcomes the identification of a high-level architecture of the system in the legislative act itself and the obligation of a reliable exchange of information as well as the need to use trust services as defined in Regulation (EU) No 910/2014.

26. There are three major recommendations the EDPS makes to ensure compliance with the Charter and the GDPR:

- providing a clear legal basis for the IT system which would be used for the transmission of documents, requests and communications for the purposes of these Regulations. In particular, in case the IT system would entail the involvement of an EU institution, body, agency or office, this legal basis should in principle be provided in an EU legislative act. Also, even in case the processing of personal data would take place in the framework of an existing IT system, the EDPS recommends providing for the use of such system in the legislative act itself. However, the existing system envisaged to be used should itself be duly established on the basis of a legal act adopted at EU level, which is currently not the case of e-CODEX. Should the EU legislator choose the e-CODEX solution, the lack of a legal instrument at EU level establishing and regulating the system should be remedied without delay.

- including in the legislative acts themselves a high level description of the IT system aspects, such as data protection responsibilities or relevant applicable safeguards, to be further defined in implementing acts. In particular, to the extent the Commission or another EU institution, body, agency or office would be implicated in the operation of the system, the legal act should ideally define its responsibilities as a (joint) controller or a processor.

- conducting an impact assessment on data protection when preparing the implementing acts.

27. The EDPS also recommends:

- providing in both legislative acts for an implementing act to further detail the IT system and that the implementing acts cover the new provisions on electronic service and on direct taking of evidence by videoconference so as to include specific safeguards also on these processing operations.

- in case of joint controllership, defining in the implementing acts the relationship among joint controllers and the content of the mandatory arrangements among them.

- specifying in the implementing acts safeguards ensuring an access to a limited number of authorised users.

- defining in further detail as far as possible the statistical elements to be collected in the implementing acts.

28. Finally, the EDPS remains at the disposal of the Commission, the Council and the European Parliament to provide advice at further stages of this process. The recommendations made in this Opinion are without prejudice to any additional comments that the EDPS could make as further issues may arise. He recalls that, in accordance with Article 42(1) of Regulation No 2018/1725, the Commission has the obligation to consult the EDPS when preparing implementing or delegated acts having an impact on the protection of individual's rights and freedoms with regard to the processing of personal data. The EDPS expects therefore to be consulted later on the provisions of the draft implementing or delegated acts in this respect.

Brussels, 13 September 2019

Wojciech Rafał WIEWIÓROWSKI

Notes

[1] OJ L 119, 4.5.2016, p. 1.
[2] OJ L 295, 21.11.2018, p. 39 (hereinafter "Regulation No 2018/1725")
[3] Proposal COM(2018)378 final (hereinafter the "taking of evidence proposal") and proposal COM (2018)379 final (hereinafter the "service of documents proposal").
[4] Explanatory memorandum, p. 2.
[5] Commission work programme 2018: an agenda for a more united, stronger and more democratic Europe (COM(2017)650 final, 24.10.2017), Annex II, points 10 and 11.
[6] Commission Staff working documents SWD(2018)285 and SWD(2018)287.
[7] Explanatory memorandum of the taking of evidence proposal, p. 3 and of the service of documents proposal, p.4:*"[w]hile in principle nothing prevents Member States from digitalising the way they communicate, past experience and projections of what will happen without EU action show that progress would be very slow and that, even where Member States take action, interoperability cannot be ensured without a framework under EU law. The objective of the proposal cannot be sufficiently achieved by the Member States themselves and can be achieved only at Union level*".
[8] P8_TA(2019)0103 and P8_TA(2019)0104.
[9] Outcome of the Council meeting (9970/19), p. 7, provisional version available at: https://www.consilium.europa.eu/media/39709/st09970-en19.pdf
According to the Presidency Paper (9566/19), par. 8 and 13, "*in the Commission Impact Assessments accompanying both proposals, e-CODEX is considered the most suitable and only readily available IT system. The development of another decentralised system would mean that the same challenges already addressed in the context of the development of the e-CODEX would be addressed once again". "One of the existing solutions is e-CODEX, a system developed with EU financial support by a consortium of Member States over a period of almost ten years. E-CODEX is currently used for the following: Business Registers Interconnection System (BRIS); the interconnection of national insolvency registers; the e-Evidence Digital Exchange System. However, insofar as use cases based on voluntary cooperation are concerned, e-CODEX is not yet implemented and used by all the Member States. In this context, during the discussions in the Working Party, for the Member States where there are currently no IT systems that support electronic procedures, the Commission could consider the development of a reference implementation solution for a back-end system at national level, provided that there is sufficiently strong and broad delegations' support for mandatory electronic communication. All systems would have to be technically interoperable and compliant with the same set of technical specifications (protocols, standards, XML schemas and workflows)."*
[10] See EDPS Opinion on the Commission Decision of 12 December 2007 concerning the implementation of the Internal Market Information System (IMI) as regards the protection of personal data (2008/49/EC), OJ 2008/C 270/01, par. 20-22: "*Based on the case-law under the ECHR, there should be no doubt about the legal status of provisions restricting fundamental rights. Those provisions must be laid down in a legal instrument, on the basis of the EC Treaty, which can be invoked before a judge. If not, the result would be legal uncertainty for the data subject since he cannot rely on the fact that he can invoke the rules before a Court.*
21. The issue of legal certainty is even more eminent since under the system of the EC Treaty it will be primarily the national judges who will have discretion to decide which value they attach to the IMI Decision. This might lead to different outcomes in different Member states and even within one Member State. This legal uncertainty is not acceptable.
22. The absence of (security about) a legal remedy would be in any event contrary to Article 6 of the ECHR which provides for the right of a fair trial, and the case law on this Article. In such a situation, the Community would not fulfil its obligations under Article 6 of the Treaty on the European Union ('TEU'), which requires the Union to respect fundamental rights, as guaranteed by the ECHR."
[11] Taking of evidence proposal, p. 6 and service of documents proposal, p. 9 and 10.
[12] OJ L 257, 28.8.2014, p. 73.
[13] Taking of evidence proposal, p. 6 and service of documents proposal, p. 9 and 10.
[14] In case of use of publicly available electronic communications services, the requirements of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37) would apply.
[15] See new Article 18a introduced by Article 1(12) of the service of documents proposal.
[16] See new Article 15a introduced by Article 1(10) of the service of documents proposal.
[17] See new Article 17a introduced by Article 1(4) of the taking of evidence proposal.

[18] See also Working Party 29 Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (wp248rev.01), footnote 21: " *When a DPIA is carried out at the stage of the elaboration of the legislation providing a legal basis for a processing, it is likely to require a review before entry into operations, as the adopted legislation may differ from the proposal in ways that affect privacy and data protection issues. Moreover, there may not be sufficient technical details available regarding the actual processing at the time of adoption of the legislation, even if it was accompanied by a DPIA. In such cases, it may still be necessary to carry out a specific DPIA prior to carrying out the actual processing activities*."
See also EDPS "Accountability on the ground Part I: Records, Registers and when to do Data Protection Impact Assessments", p. 10: "[...] *even where a DPIA according to the standards of the Regulation was carried out at the stage of the proposal for the legal basis, it would very likely require a review before entry into operations. The reason is that the adopted legal basis may differ from the proposal in ways that affect the impact on privacy and data protection. Additionally, it is usually not the case that all design choices with an impact on privacy and data protection are already determined by the legal basis. In practice, such DPIAs in the legislative process can at most be the first iteration of the DPIA process*".
[19] With regard to the proposed digitalisation measures and their impact on fundamental rights, the explanatory memorandum of the taking of evidence proposal further explains that "*the system to be introduced for electronic exchanges between the designated courts should feature a fully reliable and secure technical solution that ensures the integrity and privacy of the transmitted data. A pre-defined set of users of the system (only Member States' courts and judicial authorities) gives an additional guarantee that personal data will be handled appropriately. Furthermore, the system should introduce a decentralised structure, enabling communication directly between its end-points and thus reducing risk by minimising the number of data processors*" (p. 6. [emphasis added]). The explanatory memorandum of the service of documents proposal underlines that: "*the proposed change towards using electronic communication is expected to have an effect on the protection of personal data (Article 8 of the Charter). Technical implementation and operation of the electronic infrastructure would be determined and controlled by Member States themselves, even if the infrastructure is partially developed and financed at the EU level. The infrastructure should be based on a decentralised architecture. Data protection requirements would therefore apply exclusively at national level for the different procedures*" (p. 9. [emphasis added]). It further explains that such system "*would ensure the safe electronic communication and exchange of documents between the users of the decentralised IT system, and it would provide for automatic recording of all steps of the workflow. It would also have security features to ensure that only authorised participants with verified identities may use the system"* (p. 8).
[20] See Articles 2(2), 3 and 22 of the taking of evidence Regulation. Under the taking of evidence proposal, it is proposed to define "court" as "any judicial authority in a Member State which is competent for the performance of taking of evidence according to this Regulation" (addition of a paragraph 4 to Article 1 of the Regulation) so as to clarify that it includes for instance notaries public if empowered under national law to perform tasks of taking of evidence (explanatory memorandum, p. 8).
[21] According to Article 2 of the service of documents Regulation, these agencies are the public officers, authorities or other persons competent for the transmission of judicial or extrajudicial documents to be served in another Member State and for the receipt of such documents from another Member State. They are designated by the Member States. The information is communicated to the Commission and published on the OJEU (see Article 23 of the Regulation and Article 1(3) of the service of documents proposal inserting a new Article 3a (1)).
[22] See list of indicators in the taking of evidence impact assessment, p. 40 and the service of documents impact assessment, p. 54.