EDPS
EUROPEAN DATA PROTECTION SUPERVISOR

EDPS SUPERVISORY OPINION ON THE ROLE OF THE EUROPEAN COMMISSION IN THE PROJECT ELECTRONIC EXCHANGE OF SOCIAL SECURITY INFORMATION (EESSI)

(Case 2023-0138)

1. INTRODUCTION

1. This Supervisory Opinion regards the role of the European Commission ('the Commission') in relation to the processing of personal data in the context of the project "Electronic Exchange of Social Security Information" ('EESSI').

2. The EDPS issues this Supervisory Opinion in accordance with Article 58(3)(c) of Regulation (EU) 2018/1725[1], ('the Regulation').

2. FACTS

3. On 01 February 2023, the Commission consulted the EDPS as regards its status in relation to the processing of personal data in the context of the project EESSI.

4. On 09 March 2023, the EDPS requested additional clarifications with regard to the consultation request submitted by the Commission.

5. On 22 March 2023, an informal meeting took place between the EDPS and the Commission, where the Commission presented the legal framework and the functioning of the EESSI. On 24 March 2023, the Commission sent to the EDPS additional documentation.

[1] Regulation (EU) 2018/1725 of the European Parliament and 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, pp. 39-98.

EUROPEAN DATA PROTECTION SUPERVISOR
Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 30 - B-1000 Brussels
E-mail: edps@edps.europa.eu
Website: edps.europa.eu
Tel.: 32 2-283 19 00 - Fax: 32 2-283 19 50

6. EESSI is a **decentralised information system** set up pursuant to Regulation (EC) 883/2004[2], and Regulation (EC) 987/2009[3] to facilitate the cross-border exchange of personal data relating to social security issues between the 32 EESSI participating countries (EU member states together with EEA countries, Switzerland and the United Kingdom).[4] In particular, EESSI enables the exchange of citizens' social security claims in cases with a cross-border component. The personal data processed may include data related to sickness, accidents at work, as well as occupational diseases, unemployment benefits, family benefits, pensions and recovery of benefits.

7. The EESSI **governance** is composed of:

   i) an Administrative Commission for the Coordination of Social Security Systems, which is attached to the European Commission and is made up of government representatives from member states, and where necessary, by expert advisers ('Administrative Commission'). A representative of the Commission shall attend the meetings of the Administrative Commission in an **advisory** capacity.[5] The Commission also provides secretarial services for the Administrative Commission.[6] The Administrative Commission is mandated to adopt the common structural rules for data processing services, in particular of security and the use of standards, and [...] lay down provisions for the operation of the common parts of those services.[7]

   ii) a Technical Commission for data processing, that is attached to the Administrative Commission, and shall propose to it common architecture rules for the operation of data processing services, in particular on security and the use of standards ('Technical Commission');[8]

   iii) various ad-hoc groups, composed of national experts mandated to carry out specific tasks by the Administrative Commission.

8. With regard to the **legal basis** for the establishment of EESSI, Article 78(1) of Regulation (EC) 883/2004 provides that "*Member States shall progressively use new technologies for the exchange, access and processing of the data required to apply this Regulation and the Implementing Regulation. The European Commission shall lend its support to activities of common interest as soon as the Member States have established*

---

2 Regulation (EC) No 883/2004 of the European Parliament and of the Council of 29 April 2004 on the coordination of social security systems (OJ L 166 30.4.2004, p. 1).

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

4 For the purpose of this opinion, the wording "member states" encompasses all EESSI participating countries.

5 Article 71(1) of Regulation (EC) No 883/2004.

6 Article 71(3) of Regulation (EC) No 883/2004.

7 Article 72 of Regulation (EC) No 883/2004.

8 Article 73 of Regulation (EC) No 883/2004 of the European Parliament and of the Council of 29 April 2004 on the coordination of social security systems (OJ L 166 30.4.2004, p. 1).

such data-processing services". Furthermore, under Article 4 of Regulation (EC) 987/2009, the transmission of data between the institutions or the liaison bodies shall be carried out by electronic means, while the Administrative Commission[9] shall lay down the detailed arrangements for the exchange of documents and structured electronic documents. On the basis of the above provisions, EESSI was created to serve the purpose of carrying out exchanges of data by electronic means, replacing paper-based and other *ad hoc* existing exchanges between member states.

9. With regard to the **technical characteristics** of EESSI, its main technical elements are as follows:

   i) the **Central Service Node** (providing technical services and repositories for the overall functioning of the system), which does not contain any personal data and is hosted by the DG DIGIT data centre;

   ii) the **Access Points** (software developed by the Commission for the exchange of information among member states), hosted and fully managed by the member states. Member states share information through the Access Points. They are solely responsible for the exchanges between their Access Points and their national social security institutions. Personal data are stored in repositories by national administrations' Access Points. Although messages in transit may be stored temporarily in the DG DIGIT data centre due to technical requirements, they are never retained nor accessed by the Commission.

   iii) the **National Applications**, (they are used in EESSI to connect to the corresponding national Access Points and are used for the case management of the social security coordination cases), which fully depend on national choices. The Commission developed RINA - a case management national application that countries, which were not able to develop their own application, were free to use. The support and further development of this software had been handed over to the member states in 2021.

10. Based on the information provided by the Commission, the centrally delivered components (Central Service Node, Access Points and RINA) were developed based on requirements and specifications determined following an extensive consultation and joint work between the Commission and member states. **The specifications were approved by the Administrative Commission.**

11. With regard to the data flows taking place in the context of EESSI, the EESSI cases containing personal data of citizens, are created in a National Application of the member state concerned in a structure agreed between member states ('SED'-structured electronic document). The cases are transferred from a National

[9] See paragraph 7 on the composition of the Administrative Commission.

Application to an Access Point, via a secured communication channel ('TLS'). The exchange between Access Points is done through a highly secured network service provided by the Commission. The content of the SEDs is encrypted. The recipient Access Point decrypts the SEDs and when needed, transfers the EESSI case to a National Application of a recipient member state, via a TLS.

12. The Commission's assessment with regard to its role in the context of the processing operation in the framework of the EESSI project is that it is a processor, as the Commission solely provides a secured network through which the countries themselves exchange personal data of citizens. Such assessment has also been confirmed by the Commission Data Protection Officer ('DPO'). Nonetheless, in accordance with the information provided by the Commission, certain EESSI member states have different interpretations of their roles in the processing operation at stake.

13. Against this background, the Commission asked the EDPS to confirm whether it should be considered a processor within the meaning of Article 3(12) of the Regulation for the processing of personal data related to citizens' cases on social security coordination, as defined in Regulation (EC) No 883/2004 and Regulation (EC) No 987/2009, through the EESSI IT system.

14. In the course of the meeting that took place between the Commission and the EDPS in March 2023, the Commission clarified that its consultation request is limited to the processing of personal data related to citizens' cases on social security coordination using the EESSI IT system.[10] The EDPS notes that the Commission DPO's analysis is also limited to the latter processing operation. In that regard, the analysis below is limited to the processing operation described under paragraph 13.

15. For the sake of completeness, it is to be noted that in 2011, the EDPS issued an opinion on a notification for prior-checking received from the DPO of the Commission on the EESSI.[11] However, the Commission clarified that the prior-checking in 2011 concerned the first version of the EESSI, that was never put into production. The new version of the EESSI, where the first exchanges took place in 2019, is substantially different. Therefore, the above EDPS prior-checking opinion is no longer relevant.

[10] The EDPS asked the Commission to clarify whether its consultation request also extends to the processing of personnel data from the institutions using the EESSI IT system in the member states for the purpose of managing access/authorisation rights to parts of the EESSI IT system, as well as to the processing of personal data when the Commission provides the secretariat of the EESSI.

[11] Available at: https://edps.europa.eu/sites/edp/files/publication/11-07-28_eessi_en.pdf

3. LEGAL ANALYSIS AND RECOMMENDATIONS

16. The qualification of the Commission as a controller or a processor with regard to the processing it carries out through the EESSI IT system depends on various factors, which are outlined below.

17. In accordance with Article 3(8) of the Regulation, '**controller'** means "the Union institution or body or the directorate-general or any other organisational entity, which alone or jointly with others, **determines the purposes and means** of the processing of personal data. Where the purposes and means of such processing are determined by a specific Union act, the controller or the specific criteria for its nomination can be provided for by Union law". Therefore, unless defined in Union law, controllership is determined from an analysis of the **factual elements** or the circumstances of the case, in particular by establishing who has influence over the processing by virtue of an exercise of decision-making power.[12]

18. In other words, the identification of the 'why' and the 'how' of a processing operation is the decisive factor for an entity to assume the role of 'controller'. When carrying out a processing operation, the controller is the one deciding on the purpose ('why') and on the means to carry out such processing operation ('how'). The degree of influence of a party in determining both purposes and means may identify its role as a controller.[13]

19. With regard to the role of the **processor**, its essence lies in the processing of personal data on behalf of the controller.[14] In practice, this means that the processor is serving the interests of the controller in carrying out specific tasks, and hence, it follows the instructions set out by the controller, at least with regard to the purpose and the essential means of the processing.[15]

20. In this regard, the fact that the processor acts on behalf of the controller does not necessarily undermine its independence in carrying out specific tasks assigned to it. The processor may enjoy a considerable degree of autonomy in providing its services. However, this is due to the controller choosing to give that operational independence to the processor. Indeed, the processor may advise or propose certain measures, in particular in its field of expertise, but it is up to the controller whether to accept such advice or proposal, after having been fully informed of the

---

12 EDPB Guidelines 07/2020 of 7 July 2021 on the concepts of controller and processor in the GDPR, para 20.
13 EDPS Guidelines of 7 November 2019 on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725, p. 9-10.
14 Article 3(12) of the Regulation.
15 EDPS Guidelines of 7 November 2019 on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725, p. 16.

reasons for the measures, what the measures are and how they would be implemented.[16]

21. In this vein, it should be noted that while the determination of the purpose(s) of the processing is exclusively reserved to the controller, the processor may still determine "non-essential means of the processing", such as the choice for a particular type of hardware, software or the detailed security measures to be deployed, without assuming controllership.[17] Such elements may be identified and determined by the processor, to the extent this processing is carried out following the general instructions of the controller.[18]

3.1. Role and responsibilities of the member states

22. In the case at hand, it appears that the member states on their own or within the Administrative Commission[19] decide on the purposes and means of the processing undertaken in the context of the EESSI within the limits of the tasks assigned to them by the regulatory framework.[20] In particular, Regulation (EC) No 883/2004 mandates the Administrative Commission to adopt the common structural rules for data processing services, in particular on security and the use of standards and lay down provisions for the operation of the common part of those services.[21] Furthermore, Regulation (EC) No 987/2009 further specifies that the Administrative Commission is in charge of laying down the structure, content, format and detailed arrangements for exchange of documents and structured electronic communication.[22] Against this background, and on the basis of the information provided by the Commission, member states have decision making power over the purposes and essential means of processing, as they are in charge of :

    i) the determination of the categories of personal data that are exchanged within EESSI, as well as their storage, alteration or destruction;

---

16 EDPS Guidelines of 7 November 2019 on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725, p. 16-17.

17 EDPB Guidelines 07/2020 of 7 July 2021 on the concepts of controller and processor in the GDPR, para 40.

18 EDPS Guidelines of 7 November 2019 on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725, p. 9.

19 As explained under para 7 above, the Administrative Commission is composed of government representatives from member states, and where necessary, by expert advisers, while the European Commission attends in an advisory capacity.

20 The EDPS has no supervisory powers over member states and therefore, does not have the competence to make assessments on the role of member states in the context of processing personal data in the EESSI. Nonetheless, in the present case, the EPDS has to carry out such an assessment insofar as it is necessary to conclude on the role of the European Commission concerning processing of personal data in the context of EESSI.

21 Article 72(d).

22 Article 4(1).

ii) the determination and approval of the requirements, purpose, architecture, and specifications of the central EESSI software (Access Points);

iii) the selection of software to be used in their national domain for connection to the EESSI international domain, including whether they will use the RINA software, developed by the Commission.

23. It is also to be noted that, Article 3(3) of Regulation (EC) No 987/2009 stipulates that when collecting, transmitting or processing personal data pursuant to their legislation for the purposes of implementing the basic Regulation (i.e. Regulation (EC) No 883/2004), member states shall ensure that the persons concerned are able to exercise fully their rights with regard to data protection. This provision is an additional indication that member states are to be considered controllers of the processing operation at stake, as pursuant to Article 14(2) of the Regulation and Article 12(2) of the General Data Protection Regulation ('GDPR'), it is up to the controller to facilitate the exercise of data subject rights.[23]

3.2. Role and responsibilities of the Commission

24. With regard to the role of the Commission in the context of the EESSI project, its tasks can summarised as follows: First, the Commission is in charge of attending the meetings of the Administrative Commission in an advisory capacity[24] and providing secretarial services to it.[25] Second, it is mandated to lend its support to activities of common interest as soon as the member states have established data processing services for the exchange, access and processing of data required to apply Regulation (EC) No 883/2004 and Regulation (EC) No 987/2009.[26] In this vein, the Commission develops and maintains the EESSI technical component, provides the infrastructure for the EESSI system, ensures a secured digital communication network that enables direct connection between National Access Points, as well as the security of the system. It also proposes technical and organisational solutions in the Administrative Commission for the change requests of the system or the EESSI Common data model and implements changes when mandated by the Administrative Commission. Finally, it coordinates tests to ensure that national applications and other specific

[23] 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. 1–88.

[24] Article 71(1) of Regulation (EC) No 883/2004.

[25] Since the present opinion is limited to the role of the Commission in the context of processing of personal data related to citizens' cases on social security coordination, other functions of the Commission in the EESSI, such as the provision of secretarial services to the Administrative Commission in accordance with Article 71(3) of Regulation (EC) No 883/2004 are not examined (See also paragraphs 13 and 14 above).

[26] Article 78 of Regulation (EC) No 883/2004.

components within each member state are complied with the agreed specifications, rules and protocols.

25. In other words, the role of the Commission is limited to i) its advisory capacity, as well as ii) the maintenance of the technical components of the EESSI, and the provision of technical support in the context of EESSI. Thus, the Commission does not exercise any influence on the determination of the purpose(s) and means of the processing operation at stake, but its role is limited to the processing of personal data on behalf of the controller (i.e., member states on their own or within the Administrative Commission). The EDPS' assessment is that the Commission acts as a **processor** within the meaning of Article 3(12) of the Regulation for the processing of personal data through the EESSI IT system. Details concerning the role of the Commission in the context of the processing operation at stake are presented below.

26. With regard to its **advisory capacity**, the Commission provides recommendations to the Administrative Commission concerning the functioning of the EESSI. Such recommendations are non-binding; it is up to the member states to take the final decisions concerning how personal data are processed in the context of the functioning of the EESSI. In particular, decisions are taken by the Administrative Commission acting act by qualified majority in accordance with Article 71 (2) of the Regulation (EC) No 883/2004. In this vein, member states have the possibility to vote against the Commission's recommendations. The non-binding nature of the Commission's recommendations confirms that the Commission does not exercise any decisive influence on the processing operation at stake. The advisory role of the Commission is compatible with the role of the processor, as long as the final decision and approval on how the processing is carried out remains with controller.[27]

27. With regard to the **maintenance of the technical components of the EESSI**, and technical support in the context of EESSI, the Commission implements the decisions taken by the Administrative Commission with regard to the security of processing, the personal data to be processed, their retention period, the recipients of the personal data, etc. It also ensures a secured digital communication network enabling a direct connection between National Access Points, implements changes in the EESSI system when mandated by the Administrative Commission, and provides technical support to the EESSI system. In the context of the aforementioned activities, the Commission may recommend to member states the means of processing, such as the use of Jira software for providing help desk services. The determination of such means is subject to the approval of the member states. As underlined in the previous paragraph, the processor may advise

[27] EDPB Guidelines 07/2020 of 7 July 2021 on the concepts of controller and processor in the GDPR, para 28.

or propose certain measures to the controller, as long as it is up to the controller to accept such recommendations.

28. Furthermore, the EDPS notes that the Commission and member states have not yet formalised their relationship in the EESSI Terms of Collaboration, which is the official document describing the share of responsibility between the Commission and member states on different aspects of EESSI. Against this background, the Commission should coordinate with members to ensure that the EESSI Terms of Collaboration stipulate all the elements included under Article 29(3) of the Regulation, as well as Article 28(3) of the GDPR.

Recommendation 1: The Commission, as a processor, should ensure that it complies with its obligations under the Regulation[28], such as assisting the controller in ensuring compliance with its obligations in accordance with Article 33 to 41 of the Regulation. [29]

Recommendation 2: The Commission should coordinate with the member states to ensure that the EESSI Terms of Collaboration take into account this opinion and are in line with Article 29(3) of the Regulation and Article 28(3) of the GDPR.

4. CONCLUSION

29. In order to ensure compliance of the processing with the Regulation, the EDPS **deems necessary** that:

30. The Commission, as a processor, ensure that it complies with its obligations under the Regulation, such as assisting the controller in ensuring compliance with its obligations in accordance with Article 33 to 41 of the Regulation.

31. The Commission coordinate with the member states to ensure that the EESSI Terms of Collaboration take into account the present opinion and are in line with Article 29(3) of the Regulation and Article 28(3) of the GDPR.

[28] For instance, Article 31(2) Article 33, Article 34(2).
[29] Article 29(3)(f) of the Regulation.

32. In light of the accountability principle, the EDPS expects the Commission to implement the above recommendations accordingly and has decided to close the case.

Done at Brussels on 26 June 2023

Leonardo CERVERA NAVAS
Head of EDPS Secretariat (Acting)