



EDPS  
EUROPEAN DATA PROTECTION SUPERVISOR

# **EDPS SUPERVISORY OPINION ON THE INTEGRATION OF THE OFFICE FOR THE ADMINISTRATION AND PAYMENT OF INDIVIDUAL ENTITLEMENTS (PMO) INTO THE DIGITAL PLATFORM ELECTRONIC EXCHANGE OF SOCIAL SECURITY (EESSI) FOR THE EXCHANGE OF DATA REGARDING SOCIAL SECURITY BENEFITS (Case 2023-1346)**

## **1. INTRODUCTION**

1. This Supervisory Opinion relates to the integration of the Office for the Administration and Payment of Individual Entitlements (Paymaster Office, 'PMO') into digital platforms for the exchange of data, in particular the integration of the PMO into the digital platform "Electronic Exchange of Social Security Information" ('EESSI') for the exchange of digital data regarding social security benefits.
2. The EDPS issues this Supervisory Opinion in accordance with Articles 57(1)(g) and 58(3)(c) of Regulation (EU) 2018/1725<sup>1</sup> ('EUDPR').

---

<sup>1</sup> 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.

## 2. FACTS

3. On 13 December 2023, the European Commission ('Commission') consulted the EDPS (ref. Ares(2023)8536434) on whether existing legal bases allow the direct exchange of data regarding staff and former staff of EU institutions and other bodies by the PMO with competent institutions of Member States where such exchange is organised via Trans-European Systems<sup>2</sup>. More in particular, the Commission requested the EDPS' opinion regarding the possibility for the PMO to integrate the exchange of data regarding social security benefits via EESSI. The scope of this Opinion aligns with the latter, more specific request by the Commission.
4. The PMO is an internal Commission department responsible for the financial entitlements of staff of the Commission and certain other EU institutions<sup>3</sup>. The PMO is in charge of determining, calculating and paying out individuals' entitlements in accordance with the Staff Regulations (SR)<sup>4</sup>, the Commission Decision of 6 November 2002 establishing an Office for the administration and payment of individual entitlements<sup>5</sup>, as well as the Commission Decisions that designate the PMO as appointing authority for the provision of certain services within the Commission<sup>6</sup>.
5. A separate social security system is laid down in the SR, as foreseen in Article 14 of Protocol No 7 on the Privileges and Immunities of the European Union<sup>7</sup>. This EU social security system covers sickness benefits, maternity and equivalent paternity benefits, invalidity benefits, old-age benefits, survivors' benefits, benefits in respect of accidents and occupational diseases of active staff, unemployment benefits, pre-retirement benefits and family benefits.
6. The SR contain specific coordination rules that determine how EU social security benefits have to be coordinated with equivalent benefits from the social security

---

<sup>2</sup> As noted by the Commission in their consultation, a Trans-European System is an interoperable European solution developed for the implementation of EU law, owned by the European Commission or other bodies in support of the implementation and advancement of EU policies.

<sup>3</sup> See [https://commission.europa.eu/about-european-commission/departments-and-executive-agencies/administration-and-payment-individual-entitlements\\_en#responsibilities](https://commission.europa.eu/about-european-commission/departments-and-executive-agencies/administration-and-payment-individual-entitlements_en#responsibilities)

<sup>4</sup> Regulation No 31 (EEC), 11 (EAEC), laying down the Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Economic Community and the European Atomic Energy Community (OJ 45, 14.6.1962, p. 1385-1386).

<sup>5</sup> Commission Decision of 6 November 2002 establishing an Office for the administration and payment of individual entitlements (2003/522/EC), OJ L 183, 22.7.2003, p. 30-34.

<sup>6</sup> See Commission Decision C(2021)9126 of 15.12.2021 on the exercise of powers conferred by the Staff Regulations on the appointing authority (AA) and by the Conditions of Employment of Other Servants on the authority authorised to conclude contracts of employment (AACE).

<sup>7</sup> Protocol (No 7) on the privileges and immunities of the European Union, OJ C 326, 26.10.2012, p. 266-272, see <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2004:310:0261:0266:en:PDF>.

schemes of Member States<sup>8</sup>. In order to correctly determine rights and financial benefits, the PMO needs to process and exchange identification data and financial (social security benefits) data about its affiliates. For the time being, the PMO relies on staff and pensioners to provide the accurate information on their personal situation and social security coverage.

7. According to Article 2(2) SR, one or more institutions may entrust to any other institution or to an inter-institutional body the exercise of some or all of the powers conferred on them, as Appointing Authorities, other than decisions relating to appointments, promotions or transfers of officials. According to Article 2(4) of the Commission Decision of 6 November 2002, the PMO may act *at the request of and on behalf of* another body or agency established under or on the basis of the Treaties.
8. In the EDPS Opinion in case 2022-0528, the EDPS established that
  - where the Commission is directly mandated by the legislators to provide certain services to the EU institutions that apply the SR and the PMO is exclusively in charge of providing such services to EU institutions in accordance with the applicable regulatory framework, the PMO is to be considered a separate controller for the respective processing operations;
  - where EU institutions delegate to the PMO their competence as appointing authorities<sup>9</sup>, the PMO is a separate controller for the processing undertaken when it provides its services to EU institutions upon request on the basis of an SLA. The EU institutions in question are separate controllers for any processing operations that precede or are subsequent to the processing undertaken by the PMO in the context of the SLA.
9. As further outlined in the EDPS Opinion in case 2023-0138, EESSI is a decentralised information system set up pursuant to Regulation (EC) 883/2004<sup>10</sup>, and Regulation

---

<sup>8</sup> The Commission's consultation refers to Articles 67(2), 68(2) and 74(3) SR for national family allowance, Article 72(4) SR for sickness benefits, Articles 28a(1) in fine and Article 96(1) in fine of the Conditions of Employment of Other Servants of the European Union ('CEOS'), Article 45 of Annex VIII SR in combination with Decision 63/491/EEC for the transfer of pension rights as well as Article 43 of Annex VIII SR regarding the proof of life required from pensioners to allow the PMO to check that a pension is still payable, as the PMO may not always be informed of their death by relevant national authorities.

<sup>9</sup> According to Article 2(2) of the SR and Article 2(4) of the Commission Decision of 6 November 2002 establishing an Office for the Administration and Payment of Individual Entitlements (2003/522/EC). Such delegation of competence takes place through an AIPN delegation decision annexed to a Service Level Agreement concluded between the PMO and the EU institutions concerned.

<sup>10</sup> 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).

(EC) 987/2009<sup>11</sup> 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)<sup>12</sup>. 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.

10. In the EDPS Opinion in case 2023-0138, the EDPS established that 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)<sup>13</sup>. On that basis, the EDPS concluded 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.

### 3. LEGAL AND TECHNICAL ASSESSMENT

11. The EUDPR is applicable to processing by the PMO as internal Commission department in accordance with Article 2(1) EUDPR, since the Commission is a Union institution under Article 13 of the Treaty on European Union and therefore one of the "Union institutions and bodies" as defined in Article 3(10) EUDPR.
12. The integration of the PMO in the exchange of data via EESSI implies the transmission of data regarding social security benefits between the PMO and competent member states' authorities. Insofar as these pieces of information allow for the direct identification of natural persons, they are personal data in the sense of Article 3(1) EUDPR.

---

<sup>11</sup> 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).

<sup>12</sup> For the purpose of this opinion, the wording "member states" encompasses all EESSI participating countries.

<sup>13</sup> The Administrative Commission which is attached to the European Commission and is made up of government representatives from member states, and where necessary, by expert advisers, in accordance with Article 71 of Regulation (EC) No 883/2004.

13. Pursuant to the definition provided in Article 3(3) EUDPR, the concept of ‘processing of personal data’ designates ‘any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, ... storage, ... consultation, use, disclosure by transmission, dissemination or otherwise making available ...’. It follows that the consultation and transmission of data regarding social security benefits by the PMO via EESSI would constitute processing for the purposes of Article 3(3) EUDPR and, accordingly, falls within the scope of the EUDPR (see, in analogy, judgment of 29 January 2008, *Promusicae*, C-275/06, EU:C:2008:54, paragraph 45).
14. Article 9 EUDPR is the main data protection provision to consider when assessing whether the PMO can **transmit** data regarding social security benefits via EESSI where the **recipient** (competent national authority) is **established in the Union** (Section 3.1). In addition, any such transmission should comply with all provisions of the EUDPR, which also applies to the processing resulting from the **PMO consulting EESSI** to obtain personal data regarding social security benefits (Section 3.2).
15. As EESSI facilitates 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) and as, e.g., pensioners from EU institutions can live wherever they wish during their retirement, it cannot be excluded that the integration of the PMO in the exchange of data via EESSI leads to **international transfers** under Chapter V EUDPR (Section 3.3).

### 3.1. Article 9 EUDPR

16. Under Article 9(1)(a) EUDPR, ‘...personal data shall only be **transmitted to recipients established in the Union** other than Union institutions and bodies if...the recipient establishes that the data are necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the recipient’ (emphasis added).

#### 3.1.1. Performance of a task carried out in the public interest

17. Protocol No 7 on the Privileges and Immunities of the European Union<sup>14</sup> (‘Protocol No 7’) is the legal basis of the social security scheme for EU staff (Article 14). With regard to the sickness insurance, pension rights, family allowances and unemployment, the financial benefits of EU staff need to be coordinated with the equivalent benefits that can be granted at national level.

---

<sup>14</sup> Available at <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12012E%2FPRO%2F07>.

18. The coordination rules regarding certain social security benefits as laid down in the SR (see point 7 above) aim at the deduction of parallel benefits, which, in the light of budgetary implications, is a shared public interest of the Union and the national authorities responsible for social security benefits.
19. According to the Commission, “...*the correct deduction of allowances received from other sources and the proof of life ultimately depend on the declarations made by staff and pensioners and their dependents. Despite the legal obligation and the efforts made in terms of communication and control, it is impossible to keep track of the individual declarations of more than 80 000 beneficiaries, regardless of the resources made available...*”.
20. In the context of exchanging data on parallel benefits, the transmission of personal data regarding social security benefits via EESSI between the PMO and recipient national authorities established in the Union can thus be regarded as the performance of a task carried out in the public interest of running the social security scheme for EU staff under Article 14 of Protocol No 7 whilst safeguarding financial interests by deducing parallel benefits.

### 3.1.2. Necessity

21. Under Article 9(1)(a) EUDPR, the transmission of personal data further requires that the recipient establishes that the data are *necessary* for the performance of the task carried out in the public interest, i.e. running the social security scheme for EU staff under Article 14 of Protocol No 7 whilst safeguarding financial interests by deducing parallel benefits.
22. According to the Commission, “...*Despite the legal obligation and the efforts made in terms of communication and control, it is impossible to keep track of the individual declarations of more than 80 000 beneficiaries, regardless of the resources made available. The exchange of data with the competent institutions is the only way to limit these errors*”.
23. According to the Commission, the European Court of Auditors stated that a systemic exchange of data with the national authorities would allow reducing the risk of error resulting from the dependence on declarations made by staff and pensioners and their dependents **for** the correct deduction of allowances received from other sources and the proof of life.
24. The Commission further states that “*Cooperation with external actors makes it possible to cross-check data and find patterns based on suspected or proven fraud cases*”. According to the Commission, under the PMO Fraud Strategy, “*The PMO will explore*

*how to minimise fraud risks by establishing a systemic exchange of data with Member States”.*

25. Given Member States’ contributions to the Union budget, these attempts by the PMO to limit errors and fraud in the context of deducing parallel benefits in running the social security scheme for EU staff through exchanging personal data with the national authorities are therefore necessary in the sense of Article 9(1)(a) EUDPR.
26. The transmission of data by the PMO can be considered as necessary for the performance of a task carried out in the public interest in the in the sense of Article 9(1)(a) EUDPR. However, Article 9(1) EUDPR applies ‘without prejudice to Articles 4 to 6 and 10’.

### 3.2. Compliance with the other provisions of the EUDPR

27. The requirements of **Article 9 EUDPR** are supplementary to the conditions for lawful processing<sup>15</sup>.
28. Therefore, before the **PMO transmits** personal data regarding social security benefits to the national authorities, the PMO should also verify in particular whether the data transmission:
  - is lawful under Article 5 EUDPR;
  - complies with the data protection principles of Article 4 EUDPR.
29. The same considerations apply to the **PMO consulting EESSI** to obtain personal data regarding social security benefits.

#### 3.2.1. Legal basis laid down in Union law, Article 5 EUDPR

30. As noted above (point 26), the PMO could in principle rely on Article 5(1)(a) EUDPR, as the transmission of data by the PMO can be considered as necessary for the performance of a task carried out in the public interest in the sense of Article 9(1)(a) EUDPR. However, under Article 5(2) EUDPR, this would require that the basis for the processing shall be laid down in Union law.

##### 3.2.1.1. General requirements

31. Recital 23 EUDPR provides that “The Union law referred to in this Regulation should be clear and precise and its application should be foreseeable to persons subject to it, in accordance with the requirements set out in the Charter and the European

---

<sup>15</sup> See recital 28, last sentence EUDPR.

Convention for the protection of Human Rights and Fundamental Freedoms” (emphasis added)<sup>16</sup>.

32. According to case law of the Court of Justice of the European Union (CJEU), any legislation which entails interference with the individual rights to privacy and personal data protection must be ‘*clear and precise rules governing the scope and application of the measure in question*’<sup>17</sup>. The law must ‘*meet quality requirements: it must be accessible to the person concerned and foreseeable as to its effects*’ to guarantee that the ‘law’ permitting for an interference with fundamental rights is compatible with the rule of law<sup>18</sup> and that the individuals are protected from arbitrariness of public authorities<sup>19</sup>.
33. A legal base permitting an interference with the fundamental right to personal data protection, as in the present case, must itself define the scope of the interference with that right<sup>20</sup>. Hence, in order to serve as a legal basis for the envisaged processing operation, the Commission needs to rely on a legal basis that, as a bare minimum, clearly and specifically indicates that the PMO exchanges personal data with national authorities in the context of deducing parallel benefits in running the social security scheme for EU staff. Without such a clear and precise indication, addressees of the legal acts in question cannot reasonably foresee the applicability of specific rules interfering with their right to personal data protection.
34. Moreover, where a legal basis gives rise to a serious interference with fundamental rights to data protection and privacy, there is a greater need for clear and precise rules governing the scope and the application of the measure as well as the accompanying safeguards. Therefore, the greater the interference entailed by the legal basis, the more robust and detailed the rules and the safeguards should be.
35. In this regard, the CJEU has advanced several criteria to determine the seriousness of an interference with the right to protection of personal data and the right for respect

---

<sup>16</sup> See also the case law of the CJEU: CJEU, 22 June 2021, *Latvijas Republikas Saeima (Penalty Points)*, C-439/19, ECLI:EU:C:2021:504, §105 (‘Penalty Points’), as well as case General Court judgment of 24 February 2022, *SIA, C-175/20*, ECLI:EU:C:2022:124 (‘SIA’), §55.

<sup>17</sup> *Penalty Points*, *op.cit.*, §105, as well as *SIA*, *op.cit.*, §55.

<sup>18</sup> Case no 47143/06, *Roman Zakharov v. Russia*, 4 December 2015, *op.cit.*, §228: The Court notes from its well-established case-law that the wording ‘in accordance with the law’ requires the impugned measure both to have some **basis in domestic law and to be compatible with the rule of law**, which is expressly mentioned in the Preamble to the Convention and inherent in the object and purpose of Article 8. The law must thus meet **quality requirements: it must be accessible to the person concerned and foreseeable as to its effects** (see, among many other authorities, *Rotaru v. Romania [GC]*, no. 28341/95, §52, ECHR 2000-V; *S. and Marper v. the United Kingdom [GC]*, nos. 30562/04 and 30566/04, § 95, ECHR 2008; and *Kennedy*, cited above, §151).

<sup>19</sup> CJEU, 15 February 2016, N., *C-601/15 PPU*, EU:C:2016:84, §81.

<sup>20</sup> *SIA*, §54, and CJEU, 6 October 2020, *Privacy International*, C-623/17, ECLI:EU:C:2020:790, §65 (‘Privacy International’).



of private life. Some of the elements to be considered include (1) the nature of the personal data at issue, in particular the processing of any special categories of data<sup>21</sup>, (2) the lack of awareness of the data processing on the part of the data subject<sup>22</sup> and (3) the large-scale processing of personal data<sup>23</sup>.

36. A case-by-case assessment is necessary to assess the seriousness of the interference. In this regard, the criteria developed by the EDPS<sup>24</sup> to determine whether the processing is 'likely to result in a high risk' can also help with this assessment. Criteria relevant to the PMO's processing include in particular sensitive data processing and data processed on a large scale based on the number of people concerned. In most cases, processing meeting two or more criteria should be considered as likely amounting to a serious interference.

### 3.2.1.2. Legal bases advanced by the Commission

37. With their consultation, the Commission raises the question whether certain existing legal bases provide a sufficient legal basis for the PMO to allow the direct exchange of social security data regarding staff and former staff of EU institutions and other bodies with competent institutions of Member States where such exchange is organised via Trans-European Systems, in the case at hand via EESSI.

38. In this context, the Commission refers to the following potential legal bases (see section 4.2 of the consultation):

- Protocol No 7, which provides the general legal framework for the transmission of data on EU staff to the Member States and is the legal basis of the social security scheme of EU staff. The coordination rules regarding certain social security benefits as laid down in the SR require the exchange of data on parallel benefits, which can be granted by the Member States.
- Regulation (EC) No 987/2009<sup>25</sup>, which according to the Commission “...holds provisions which provide the legal basis for the exchange of data regarding social security benefits between the competent institutions of the Member States. It is

---

<sup>21</sup> Judgment of the Court of 11 December 2019, *Asociația de Proprietari bloc M5A-ScaraA*, C-708/18, EU:C:2019:1064, §§57-63

<sup>22</sup> See e.g. *Tele2 Sverige and Watson and Others*, §117.

<sup>23</sup> See e.g. *La Quadrature du Net and Others*, §119.

<sup>24</sup> See Annex 1 of the Decision of the EDPS of 16 July 2019 on DPIA lists issued under Articles 39(4) and (5) of the Regulation (EU) 2018/1725.

<sup>25</sup> *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.*

*also the legal basis for EESSI, the Electronic Exchange of Social Security Information, which is progressively being implemented...”;*

- According to the Commission, Regulation (EU) No 1024/2012<sup>26</sup> in combination with Regulation 2018/1724<sup>27</sup> could be considered to constitute the necessary legal basis for the direct digital exchange of data with other IMI actors included in the Single Digital Gateway, and more in particular with the competent institutions of EU Member States in charge of the management of social security benefits, since the EU institutions and bodies have been qualified as IMI actors and are included in the Single Digital Gateway.

### 3.2.1.3. Protocol No 7

39. Whilst it is correct to state that the coordination rules regarding certain social security benefits as laid down in the SR require the exchange of data on parallel benefits, which can be granted by the Member States, Protocol No 7 as well as the SR are silent on the means of such exchange.
40. In addition, Article 15(2) of Protocol No 7 referring to the transmission of personal data to EU Member States limits this transmission to the *periodical* communication of *limited categories* of personal data (names, grades and addresses of officials and other servants of the Union to whom Article 11, the second paragraph of Article 12, and Article 13 shall apply, in whole or in part).
41. Protocol No 7 and the SR are thus not a sufficient legal basis for the direct exchange of social security data organised via Trans-European Systems, in the case at hand via EESSI.

### 3.2.1.4. Regulation (EC) No 987/2009

42. Regulation (EC) No 987/2009<sup>28</sup>, which is based inter alia on Article 89 of Regulation (EC) No 883/2004<sup>29</sup>, holds provisions, which provide the legal basis for the exchange of data regarding social security benefits *between the competent institutions of the*

---

<sup>26</sup> Regulation (EU) No 1024/2012 on administrative cooperation through the Internal Market Information System and repealing Commission Decision 2008/49/EC (‘the IMI Regulation’), OJ L 316, 14.11.2012, p. 1–11, see <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32012R1024>.

<sup>27</sup> Regulation (EU) 2018/1724 of the European Parliament and of the Council of 2 October 2018 establishing a single digital gateway to provide access to information, to procedures and to assistance and problem-solving services and amending Regulation (EU) No 1024/2012, OJ L 295, 21.11.2018, p. 1–38.

<sup>28</sup> 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. 1–42

<sup>29</sup> 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.

*Member States. As explicitly noted by the Commission, “EU staff do not come under the personal scope of the Coordination Regulations as defined in Article 2 of Regulation (EC) No 883/2004, the EU institutions and bodies have not as yet been explicitly included into EESSI”.*

43. The Commission brings forward that, at the start of the EESSI development, the inclusion of EU institutions and bodies had implicitly, if not explicitly been foreseen. The Commission notes that *“It was foreseen that exchanges related to assessing eligibility to unemployment benefit of EU staff could be done via EESSI”* and refers, in this context, to Commission Regulation (EC) No 780/2009<sup>30</sup>.
44. In its recital 5, Commission Regulation (EC) No 780/2009 indeed states *“Exchanging information electronically, particularly under the EESSI (Electronic Exchange of Social Security Information) project, is one way to increase the effectiveness of cooperation between the Commission and the competent national authorities with responsibility for employment and unemployment”*. However, this is provided only in a non-binding recital and does not have a corresponding legal provision in the enacting terms of Commission Regulation (EC) No 780/2009.
45. At any rate, this would only cover *exchanges related to assessing eligibility to unemployment benefit of EU staff*, i.e. not all types of exchanges of social security related data envisaged under the consultation.
46. In the light of the above, Regulation (EC) No 987/2009 is not a sufficient legal basis for the direct exchange organised via Trans-European Systems, in the case at hand via EESSI.

### 3.2.1.5. Regulation (EU) No 1024/2012 in combination with Regulation 2018/1724

47. According to the Commission, *“Since the EU institutions and bodies have been qualified as IMI actors and are included in the Single Digital Gateway, the IMI Regulation 2012/1024 juncto Regulation 2018/1724 could be considered to constitute the necessary legal basis for the direct digital exchange of data with other IMI actors included in the Single Digital Gateway, and more in particular with the competent institutions of EU Member States in charge of the management of social security benefits.”*

---

<sup>30</sup> Commission Regulation (EC) No 780/2009<sup>30</sup> of 27 August 2009 laying down provisions for implementing the third subparagraph of Article 28a(2) and the third subparagraph of Article 96(2) of the Conditions of Employment of Other Servants of the European Communities (CEOS), OJ L 226, 28.8.2009, p. 3–7.

48. Under recital 4 of Regulation (EU) No 1024/2012<sup>31</sup>, the purpose of IMI should be to improve the functioning of the internal market by “*providing an effective, user-friendly tool for the implementation of administrative cooperation between Member States and between Member States and the Commission, thus facilitating the application of Union acts listed in the Annex to this Regulation*”.
49. No Union act on the direct digital exchange of data by the PMO with the competent institutions of EU Member States in charge of the management of social security benefits is listed in the Annex of Regulation (EU) No 1024/2012.
50. Regulation (EU) No 1024/2012 can thus, on its own, not be considered a sufficient legal basis for the direct exchange organised via Trans-European Systems, in the case at hand via EESSI.
51. Regarding a possible combination with Regulation (EU) 2018/1724, the EDPS notes that recital 40 of Regulation (EU) 2018/1724 refers to allowing Union bodies, offices or agencies to become actors within IMI.
52. However, recital 30 of Regulation (EU) 2018/1724 explicitly excludes procedures applicable in the field of social security coordination from the scope of the Regulation<sup>32</sup>.
53. In the light of the above, Regulation (EU) No 1024/2012 in combination with Regulation (EU) 2018/1724 cannot be considered as legal basis for the PMO to allow the direct exchange of social security data organised via Trans-European Systems, in the case at hand via EESSI.
54. The EDPS **deems necessary** that the Commission establish an explicit legal basis for the PMO to allow the direct exchange of social security data organised via Trans-European Systems, in the case at hand via EESSI. Against that background, the EDPS welcomes that, according to the Commission, the imminent consultation of the Legal Service will provide greater clarity in the context of the Commission’s current work on a draft Regulation to clarify the legal basis for data exchanges with Member States in the context of PMO.

---

<sup>31</sup> Regulation (EU) No 1024/2012 on administrative cooperation through the Internal Market Information System and repealing Commission Decision 2008/49/EC (“the IMI Regulation”), OJ L 316, 14.11.2012, p. 1–11, see <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32012R1024>.

<sup>32</sup> “This Regulation should not affect the social security coordination rules set out in Regulations (EC) No 883/2004 and (EC) No 987/2009 of the European Parliament and of the Council, which define the rights and obligations of insured persons and social security institutions, as well as the procedures applicable in the field of social security coordination.”

### 3.2.2. Data protection principles, Article 4 EUDPR

55. Under the accountability principle (Article 4(2) EUDPR), the controller shall be responsible for, and be able to demonstrate compliance with the data protection principles listed in Article 4(1) EUDPR.

#### 3.2.2.1. Controllership, Article 4(2)

56. Under the accountability principle (Article 4(2) EUDPR), it is the **controller's** responsibility to ensure and be able to demonstrate compliance with the data protection principles.

57. When it comes to the direct exchange of social security data via EESSI by the PMO, the Commission notes with reference to the EDPS Opinion in case 2022-0528 (§26) that *“The EDPS confirmed that the PMO is a separate controller within the meaning of Article 3(8) of the EUDPR with regard to the processing of personal data it undertakes in the context of the provision of the services that it renders to EU institutions.”*

58. The Commission also refers to the EDPS Opinion in case 2023-0138 and states that *“The roles of the Commission being processor and the Member States being controllers and for some parts processors within the EESSI system is confirmed by an EDPS opinion”*.

59. Against that background, the Commission concludes that *“A logical consequence of these roles is that the processing of personal data undertaken by PMO as a data controller via EESSI, for which the Commission is confirmed to be a data processor, would be regulated by an agreement between these two entities, as foreseen by Article 29 of EUDPR”* and mentions that *“DG EMPL is currently discussing such a processor/controller agreement with the Member States in the frame of the relevant governance bodies of EESSI”*.

60. In the light of these statements, the EDPS would like to note that the EDPS Opinion in case 2022-0528 applies to cases (i) where the Commission is directly mandated by the legislators to provide certain services to the EU institutions (not the case here) or (ii) where EU institutions delegate to the PMO their competence as appointing authorities<sup>33</sup> (not the case here either).

61. For services rendered by the PMO as the internal Commission department responsible for the financial entitlements of staff of the Commission *to the*

---

<sup>33</sup> According to Article 2(2) of the SR and Article 2(4) of the Commission Decision of 6 November 2002 establishing an Office for the Administration and Payment of Individual Entitlements (2003/522/EC). Such delegation of competence takes place through an AIPN delegation decision annexed to a Service Level Agreement concluded between the PMO and the EU institutions concerned.

*Commission*, the controller remains the Commission, not PMO. This is because in accordance with Article 2 of the Commission Decision (EU) 2020/969<sup>34</sup>, “(...) the Commission shall be considered to be the controller within the meaning of Article 3(8) of Regulation (EU) 2018/1725”. At the same time, the Head of a Directorate-General, Service or Cabinet, which carries out a processing operation on behalf of the Commission in fulfilment of the mission of the Directorate-General, Service or Cabinet, is to be considered a “delegated controller” in accordance with Article 3(4) of the above Commission Decision. Therefore, in accordance with the above decision, the PMO would be considered a “delegated controller”.

62. When the PMO (as internal Commission department, i.e. as Commission) integrates EESSI for the exchange of social security data, the role of the Commission might no longer be 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.
63. Insofar as the Commission (PMO as internal Commission department) as a user of EESSI can exercise any influence on the determination of the purpose(s) and means of the processing operation at stake through the governance structure of EESSI (e.g. within the Administrative Commission), the Commission’s role would no longer be limited to the processing of personal data on behalf of the controller (i.e., member states on their own or within the Administrative Commission).
64. It would consequently cease to be a mere processorship *in the specific context* of PMO integrating EESSI for the exchange of social security data.
65. In this context, the EDPS takes note of the fact that “*DG EMPL is currently discussing... a processor/controller agreement with the Member States in the frame of the relevant governance bodies of EESSI*” and **recommends** evaluating and, where appropriate, taking into account the need to differentiate the potentially controlling role of the Commission in this context.

### 3.2.2.2. Lawfulness, Articles 4(1)(a) and 10(2)(b) EUDPR

66. Under Article 4(1)(a) EUDPR, personal data shall be processed **lawfully**, fairly and in a transparent manner.
67. The exchange of social security data will involve processing of data concerning health (e.g. in cases related to sickness benefits or family members dependent for health

---

<sup>34</sup> Commission Decision (EU) 2020/969 of 3 July 2020 laying down implementing rules concerning the Data Protection Officer, restrictions of data subjects’ rights and the application of Regulation (EU) 2018/1725 of the European Parliament and of the Council, and repealing Commission Decision 2008/597/EC, OJ L 213, 6.7.2020, p. 12–22.

reasons) and, potentially, data concerning a natural person's sex life (e.g. in the context of family allowances).

68. Under Article 10(2)(b) of the Regulation, this is permitted insofar as the processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller in the field of employment and social security and social protection law insofar as it is authorised by **Union law providing for appropriate safeguards for the fundamental rights and the interests of the data subject** (emphasis added).
69. For the need to establish an explicit legal basis for the PMO to allow the direct exchange of social security data organised via Trans-European Systems, in the case at hand via EESSI, see above Section 3.2.1.
70. In the light of Article 10(2)(b) EUDPR, the EDPS **deems necessary** that, when establishing an explicit legal basis for the PMO to allow the direct exchange of social security data via EESSI, the Commission ensure appropriate safeguards for the fundamental rights and the interests of the data subjects concerned<sup>35</sup>.

### 3.2.2.3. General compliance with the data protection principles

71. As noted above, under the accountability principle (Article 4(2) EUDPR), the controller shall be responsible for, and be able to demonstrate compliance with the data protection principles listed in Article 4(1) EUDPR.
72. In addition, the controller has to design processes in a way that ensures they are compliant with the rules (see Articles 4(2) and 26 EUDPR). Under Article 26 EUDPR, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation 'taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons'.
73. The consultation states that "*The exchange of data via digital platforms is being put in place with the support and under the supervision of Commission services and are GDPR compliant by default and by design. ...These platforms were created with the support of the European Commission and are in strict compliance with the GDPR. They can be considered as being in compliance with the EUDPR with regard to the direct exchange of personal data between the competent services of the EU institutions and other bodies and*

---

<sup>35</sup> For further guidance, see e.g. the [EDPS Supervisory Opinion in case 2021-0830](#).

*the competent services of the Member States. The data exchange also complies with the necessity and proportionality principles of article 9 (1) and (2) of the EUDPR.”*

74. It also notes that “*Exchanging data directly with the competent institutions via a secure electronic system improves the data protection compared to ad hoc transmissions or transmissions via the data subject, by limiting the number of intermediaries, streamlining the communication channels, reducing the risk of data breaches, and increasing transparency.*”
75. The Commission did not share any respective documentation of their above assessments, in particular no assessment of EESSI (or any other platform) “*being in compliance with the EUDPR with regard to the direct exchange of personal data between the competent services of the EU institutions and other bodies and the competent services of the Member States*”.
76. As is clear from Article 4 EUDPR (entitled “Principles relating to processing of personal data”) and the definition of ‘processing’ under Article 3(3) EUDPR, the obligation to ensure and demonstrate compliance applies to *processing operations* involving personal data (i.e. to the envisaged exchange of social security data between the PMO and Member States), not only to *individual tools applied in that context* (in the case at hand, EESSI)<sup>36</sup>.
77. In view of the controller’s obligations under Articles 4(2) and 26 EUDPR as well as in the light of the requirements under Article 10(2)(b) EUDPR and the the “*more than 80 000 beneficiaries*” concerned, the EDPS **recommends** conducting a holistic compliance and risk check of the envisaged processing operation (exchange of social security data between the PMO and Member States) as further outlined in EDPS guidance<sup>37</sup>.
78. In this context and in the light of the data minimisation principle under Article 4(1)(c) EUDPR, the EDPS **recommends** looking into hit/no hit systems for achieving the purpose pursued by the PMO, i.e. to limit errors and fraud in the context of deducing parallel benefits in running the social security scheme for EU staff (see above point 26).

### 3.3. International transfers under Chapter V EUDPR

79. As EESSI facilitates the cross-border exchange of personal data relating to social security issues between the 32 EESSI participating countries (EU Member States

---

<sup>36</sup> See EDPS guidance “[Accountability on the ground: Guidance on documenting processing operations for EU institutions, bodies and agencies \(EUIs\)](#)”.

<sup>37</sup> See EDPS guidance “[Accountability on the ground: Guidance on documenting processing operations for EU institutions, bodies and agencies \(EUIs\)](#)”, in particular section 3.2 and Annex 2.



together with EEA countries, Switzerland and the United Kingdom) and as, e.g., pensioners from EU institutions can live wherever they wish during their retirement, it cannot be excluded that the integration of the PMO in the exchange of data via EESSI leads to international transfers under Chapter V EUDPR.

80. The EDPS recalls that, under Article 46 EUDPR, any transfer of personal data to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor.
81. Under Article 47(1) EUDPR, a transfer of personal data to a third country or international organisation may take place where the Commission has decided pursuant to Article 45(3) of Regulation (EU) 2016/679 that the third country in question ensures an adequate level of protection and where the personal data are transferred solely to allow tasks within the competence of the controller to be carried out. Currently, transfers to Switzerland and the United Kingdom occurring in the context of the processing operation at hand are covered by respective adequacy decisions<sup>38</sup>.
82. The EDPS **recalls** that, under Article 47(3) EUDPR, the Commission shall take the necessary measures to comply with decisions establishing that a third country or one or more specified sectors within a third country no longer ensures an adequate level of protection.

## 4. CONCLUSION

83. The transmission of data by the PMO can be considered as necessary for the performance of a task carried out in the public interest in the in the sense of Article 9(1)(a) EUDPR.
84. The potential legal bases brought forward by the Commission in the consultation cannot be considered as legal basis for the PMO to allow the direct exchange of social security data organised via Trans-European Systems, in the case at hand via EESSI.

---

<sup>38</sup> Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland, OJ L 215, 25.8.2000, p. 1–3, and Commission Implementing Decision (EU) 2021/1772 of 28 June 2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom, OJ L 360, 11.10.2021, p. 1–68, respectively.

85. Insofar as the Commission (PMO as internal Commission department) as a user of EESSI can exercise any influence on the determination of the purpose(s) and means of the processing operation at stake through the governance structure of EESSI (e.g. within the Administrative Commission), the Commission's role would no longer be limited to the processing of personal data on behalf of the controller (i.e., member states on their own or within the Administrative Commission).
86. Under Article 47(3) EUDPR, the Commission shall take the necessary measures to comply with decisions establishing that a third country or one or more specified sectors within a third country no longer ensures an adequate level of protection.

As indicated above, in order to ensure compliance of the processing with the Regulation, the EDPS **deems necessary** that the Commission:

1. establish an explicit legal basis for the PMO to allow the direct exchange of social security data organised via Trans-European Systems, in the case at hand via EESSI;
2. when establishing such explicit legal basis, ensure appropriate safeguards for the fundamental rights and the interests of the data subjects concerned.

Moreover, the EDPS **recommends** that the Commission:

3. evaluate and, where appropriate, take into account the need to differentiate the potentially controlling role of the Commission in the context of the processing operation at hand when discussing a processor/controller agreement with the Member States in the frame of the relevant governance bodies of EESSI;
4. conduct a full-fledged and holistic compliance and risk check of the envisaged processing operation. In this context, the Commission should look into hit/no hit systems for achieving the purpose pursued by the PMO, i.e. to limit errors and fraud in the context of deducing parallel benefits in running the social security scheme for EU staff.

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 5 February 2024

*[e-signed]*

Wojciech Rafał WIEWIÓROWSKI