



## **Opinion on a notification for prior-checking received from the Data Protection Officer of the European Commission on the Electronic Exchange of Social Security Information system ("EESSI")**

Brussels, 28 July 2011 (Case 2011-0016)

### **1. Proceedings**

On 5 January 2011, the European Data Protection Supervisor ("EDPS") received from the Data Protection Officer ("DPO") of the European Commission a notification for prior checking concerning the Electronic Exchange of Social Security Information system ("EESSI"). This is a true prior checking; according to the implementation planning, it is foreseen that EESSI would start being operational towards the end of the transitional period by 1 May 2012.

#### **1.1. Prerequisites for the establishment of EESSI**

EESSI is an information system created by the EU that can be considered as a large scale IT system since it involves cross-border exchanges of a certain amount of personal data on social security between all Member States. EESSI has therefore considerable impact on the privacy and data protection of individuals.

The impact of such a large scale IT system on the privacy and data protection of individuals shall be assessed at two levels: (1) at the legislative level, pursuant to Article 28(2) of Regulation (EC) No 45/2001, the EDPS should be consulted on the proposed EU legislative measure introducing such a large-scale IT system; (2) at the implementing level, the national data protection authorities in Member States, and the EDPS in respect of the processing carried out by EU institutions and bodies, must be appropriately notified of the data processing.

The EDPS notes with satisfaction that, pursuant to Article 28(2) of Regulation (EC) No 45/2001, he was consulted by the Commission on the draft implementing Regulation on the coordination of social security systems, which is the legal basis providing for the technical details of EESSI. In his consultative Opinion<sup>1</sup>, the EDPS provided comments on the legal framework for the implementation of EESSI and highlighted specific issues which require taking appropriate actions from a data protection viewpoint. Some of the issues were addressed in the implementing Regulation itself, the final version of which incorporates some of the suggestions made by the EDPS; others require further implementing steps by Member States and/or the Commission.

The EDPS therefore underlines that the present prior checking Opinion, which assesses the implementing measures notified to him by the Commission, should be considered jointly with the consultative Opinion.

<sup>1</sup> Opinion of the EDPS on the Proposal for a Regulation of the European Parliament and of the Council laying down the procedure for implementing Regulation (EC) No 883/2004 on the coordination of social security systems (COM (2006)16 final), adopted on 6 March 2007.

## 1.2. Deadline for the Opinion

Pursuant to Article 27(4) of Regulation (EC) No 45/2001, this Opinion must be delivered within two months, discounting any periods of suspension allowed for receipt of additional information requested by the EDPS. The EDPS requested further information from the Commission on 17 February 2011. These were provided on 3 March 2011 and 6 April 2011, respectively. The deadline for issuing the Opinion was initially set on 26 April 2011 (April 24 being a Saturday and Monday 25 Easter holiday). However, given the complexity of the case, the deadline was extended by one month in accordance with Article 27(4) of the Regulation. Further questions were asked on 28 April, which were discussed during a meeting between EDPS staff and DG EMPL staff held on 22 June 2011. Further clarifications were provided in writing on 6 July 2011 and on 8 July 2011. The EDPS sent his draft Opinion for comments on 18 July 2011, which were received on 27 July 2011. The procedure was suspended for a total of 182 days. Consequently, the present Opinion must be delivered no later than on 14 August 2011.

## 2. Facts

**EESSI** is an ICT system connecting Member States' administrations in charge of social security for electronic data exchanges. It has been developed by the European Commission pursuant to Regulation (EC) No 883/2004 as amended by Regulation (EC) No 988/2009 (the "basic Regulation") and Regulation (EC) No 987/2009 (the "Implementing Regulation") on social security coordination.

**Scope of EESSI:** From a geographical perspective, the EU rules on social security coordination apply not only within the EU territory but also in a number of participating countries<sup>2</sup>, namely Iceland, Liechtenstein, Norway and Switzerland. The EU rules on social security coordination apply to nationals of EU Member States and participating countries as well as nationals of third countries legally resident in the EU having worked in more than one EU Member States. Data exchanges will take place between competent administrations of all participating countries in the areas governed by the Regulations on social security coordination, namely:

- sickness, maternity and equivalent paternity benefits
- old-age pensions, pre-retirement and invalidity benefits
- survivors' benefits and death grants
- unemployment benefits
- family benefits
- benefits in respect of accidents at work and occupational diseases

The **purpose** of EESSI is to strengthen the protection of citizens' rights by enabling the electronic exchange of personal social security information on migrant workers in the EU among Member States' competent administrations. The aim is that the 200 paper forms currently used for communication between administrations should be superseded by EESSI. IT-based exchanges in EESSI will notably (i) facilitate and speed up the decision-making for the calculation and payment of social security benefits; (ii) allow a more efficient verification of data; (iii) provide a more flexible and user-friendly interface between different systems; and (iv) provide an accurate collection of statistical data on European exchanges.

---

<sup>2</sup> For convenience, this Opinion will only refer to "Member States". However, the reference in this Opinion to "Member States" shall be understood to also include EEA countries (Iceland, Liechtenstein, Norway) and Switzerland.

**Time line:** The Regulations on social security coordination have entered into force on 1 May 2010; however a transitional period of two years has been agreed upon to allow Member States to connect their national applications to the EESSI system. By 1 May 2012, all administrations should be connected to and be exchanging information via EESSI.

#### **Data controllers: roles and responsibilities**

The operation of EESSI involves shared responsibilities between Member States and the Commission:

- **At the Member States level,** personal data are collected by competent administrations of the Member States in accordance with the national data protection rules implementing Directive 95/46/EC. Each competent administration is responsible for its own processing of the data and for the exchange of personal data in EESSI in accordance with the rules set forth in Articles 77<sup>3</sup> and 78<sup>4</sup> of the basic Regulation. Under Directive 95/46/EC, competent administrations dealing with social security can be identified as data controllers and have therefore relevant duties and responsibilities.
- **Role of the Commission in determining the purposes and means of the processing in EESSI:** According to the notification submitted to the EDPS, the Commission is a controller in respect of its role in EESSI. The Commission is responsible for the coordination of EESSI, it assures the Secretariat of the EESSI Project Steering Committee and participates, in an advisory capacity, in the Administrative Commission for the Coordination of Social Security Systems (the "Administrative Commission")<sup>5</sup>. The Commission is also responsible for the central infrastructure and for ensuring the security of the data exchanged. As a result the European Commission shares some responsibilities and duties with respect to EESSI as controller under Regulation (EC) No 45/2001. In addition, the Commission is also the controller<sup>6</sup> of the public database that will be created pursuant to Article 88(4) of the Implementing Regulation, on which will be listed

---

<sup>3</sup> Article 77 provides that *"Where, under this Regulation or under the Implementing Regulation, the authorities or institutions of a Member State communicate personal data to the authorities or institutions of another Member State, such communication shall be subject to the data protection legislation of the Member State transmitting them. Any communication from the authority or institution of the receiving Member State as well as the storage, alteration and destruction of the data provided by that Member State shall be subject to the data protection legislation of the receiving Member State. Data required for the application of this Regulation and the Implementing Regulation shall be transmitted by one Member State to another Member State in accordance with Community provisions on the protection of natural persons with regard to the processing and free movement of personal data."*

<sup>4</sup> Article 78(2) notably provides that *"Each Member State shall be responsible for managing its own part of the data-processing services in accordance with the Community provisions on the protection of natural persons with regard to the processing and the free movement of personal data."*

<sup>5</sup> The Administrative Commission is attached to the European Commission and is the main governance body in the field of EU social security coordination. It is composed of representatives of all participating countries as well as a representative from the European Commission. The decisions taken in this Administrative Commission in respect of the implementation of EESSI concern all policy, organizational and technical aspects related to the deployment, implementation and operation of the system. For example, the Administrative Commission decided on the content and format of the electronic structured documents (SEDs). In respect of the data processing, it takes on the advice of the Technical Commission on Data Processing.

<sup>6</sup> The processing activities carried out by the Commission in relation to the provision of EESSI directory services are not as such subject to prior checking by the EDPS. However, considering that they are an essential component of EESSI, these processing activities are described in this Opinion.

the relevant competent administrations for each Member State and their contact points.

- **Future role of the Commission as user of the system:** while such role is not envisaged in the first roll out of EESSI, in the longer term it is foreseen that the Commission (PMO) will become a user of EESSI as a competent administration. The relevant department in the Commission having responsibility for such processing will be the data controller of such processing and will have relevant duties and responsibilities under Regulation (EC) No 45/2001. Such role will require submitting to the EDPS a separate prior checking notification; it is therefore not described nor analysed in the present Opinion.

The **primary responsibility** for the processing undertaken by the Commission for purpose of operating the EESSI infrastructure lies with the Unit "Coordination of social security schemes, free movement of workers", at DG Employment, Social Affairs and Inclusion (DG EMPL, B.4). In the frame of the standard working practices in DG EMPL, Unit B.4 is supported by Unit G.4 with respect to technical IT knowledge, expertise and support. Unit G.4 is responsible for the development, maintenance and support of the system that will support the electronic exchange of messages.

**Data processor:** The Commission has appointed the Commission DIGIT Data Centre as **processor**. The Commission DIGIT Data Centre hosts and operates central components of EESSI (in particular the sTESTA infrastructure which serves as a communication network connecting Member States' national networks among themselves and with the DIGIT Data Centre). It dispatches information and collects statistics. A hosting proposal was agreed between DG EMPL and DIGIT for the operation of central EESSI infrastructure hosted at the Commission DIGIT Data Centre. A Service Level Agreement between DG EMPL and DIGIT is in the course of being finalised. A draft of the standard SLA was provided to the EDPS; page 9 of the standard SLA contains data protection clauses implementing Article 23 of the Regulation.

**Description of the processing:** Personal data are collected by local, regional and national administrations and then transmitted via EESSI to competent administrations in other Member States through a common secure network. A common European architecture for the electronic exchange of data was defined by the Administrative Commission, which main features are as follows:

**EESSI high level architecture:** The system is designed as a "star" topology with a central Coordination Node (CN) and with end-points called Access Points (AP), which are deployed in the Member States. EESSI consists in essence of (i) a central unit (the Coordination Node) to be hosted in the Commission's DIGIT Data Centre and including the EESSI directory services, and (ii) the international parts of APs of the Member States which are connected via a safe network (sTesta) with the Coordination Node and through which all electronic data have to be exchanged between Member States.

The common EU infrastructure is developed at EU level whereas the Member States are responsible to take the necessary steps in order to be connected to the whole system. To that end, Member States have designated at least one and maximum five access points, through which the data are transmitted between the Member States. EESSI only concerns the exchange of information between Member States via their access points. The transmission of data from the national parts of the access point(s) to the national social security institutions remains entirely within the competence of the Member States.

EESSI AP\_RI and WEBIC (Web interface for clerks): The Commission developed a reference implementation software, which Member States may use on a voluntary basis. The reference implementation includes a pre-defined international and national access point (the AP\_RI) and a default Web Interface for Clerks (the WEBIC).

SEDs messages and flows: The exchange of social security information is done by structured electronic documents (SEDs) to be exchanged according to a business protocol. Both message structure and protocol are approved by the relevant steering committees and working groups. The SEDs can only be exchanged within predefined work flows. To that end, about 100 flows have been defined within which the SEDs can be exchanged. These flows are the translation of the information exchange processes between administrations which are defined by the Implementing Regulation. Flows can only be exchanged between two competent administrations; if data must be sent to several recipients, the sending administration must repeat the operation as many times as there are recipients. There cannot be any sending of data to all recipients.

Search functions in EESSI: It is possible for clerks of competent administrations to search flows of information taking place through EESSI. They will have access to the headers of all flows, but will only be able to access the content of a particular SED message if they are authorised to do so, i.e. they are the sender/ designated recipient of such flow.

EESSI central directory<sup>7</sup>: A central directory hosted in the Commission's data Centre contains information related to the social security administrations. The central directory processes contact details of administrations as well as personal data of contact persons at competent administrations. This directory will be used:

- By the APs to retrieve the recipient AP's address. For that purpose a replication of the master directory is periodically transmitted to the APs.
- By the CN to validate the AP's address while relaying the SED messages.
- By the civil servants in the Member State administrations to identify administrations in other Member State (using the AP's local replication of the master directory).
- By the European Citizens to get information about administrations via the EESSI public website (using a replication of the master directory named "public directory").

Information repository: There will be an information repository to disseminate general EESSI information to stakeholders (e.g. EESSI model documentation, design documents, software updates, etc.).

**Data subjects** are workers, and their family members, having worked in more than one of the Member States and claiming for social security benefits<sup>8</sup>. The Regulations on social security also coordinate the social security rights of non-active persons who have links with more than one of the Member States. The Regulations also apply to nationals of third countries legally resident in the EU, pursuant to Council Regulation (EC) No 1231/2010<sup>9</sup>.

---

<sup>7</sup> See footnote 6.

<sup>8</sup> It is foreseen that, in the future, EU civil servants and other categories of staff working for EU institutions and bodies will also become data subjects in EESSI. This Opinion will not deal with such aspects, which will be analysed separately when a notification for prior checking is submitted to the EDPS by the relevant EU controller concerning its processing activity as a competent administration in EESSI.

<sup>9</sup> Regulation (EU) No 1231/2010 extending the provisions of Regulation (EC) No 883/2004 and Regulation (EC) No 987/2009 to nationals of third countries who are not already covered by those provisions solely on the ground of their nationality.

**Personal data exchanged in EESSI:** Specific provisions of the basic Regulation define the scope of the personal data that need to be exchanged between competent administrations. An EESSI model has been agreed upon in working groups set up by the Administrative Commission, which defines the content of the data to be exchanged in SEDs and the flow types. In total, 350 SEDs have been defined. A review of the SEDs shall take place after a certain experience has been gained with the use of the SEDs and flows. Depending on the claimed social security benefit and other factors, the following types of personal data may be exchanged through EESSI:

- Name, sex, address, birth date and place, residence information, family status, family composition and identities (including e.g. children adoption) of current and deceased members, social security entitlement info (social security ID, PIN (Personal Identification Number) in the relevant social security administration, start, end, possible refusal reasons etc.), information on patient's health (including e.g. medical exams/treatments) and accidents, information on benefits enjoyed, financial information (including bank account, fiscal identification and trade register numbers, income), employment status and employment record (including reason for termination). Data revealing sexual orientation may, in certain cases, be derived from the civil status.

**Data transfers:** The recipients of the data exchanged through EESSI will be the clerks of competent Member States administrations in the relevant specific sector of social security. The Commission ensures the exchange of personal data between Member States but shall not have access to the content of the personal data that will transit through EESSI encrypted (the Commission can only access headers of messages for statistical purposes, as explained below). DIGIT staff have access to certain technical data used by the messaging system in their capacity of EC administrators of the coordination node for purpose of managing the coordination node and for gathering statistics. Staff of DG EMPL, G.4, have access to certain data in EESSI in their capacity of EC Administrator<sup>10</sup> and DS Administrator<sup>11</sup> of the EESSI central directory.

Data subjects have **the right to access to their data and to rectify them** by contacting the local, regional or national administration where they made their social security benefit claim or any other national competent authority they are addressed to. According to the social security regulations, it is the Member States' responsibility to ensure that data subjects are able to exercise fully their rights regarding personal data protection. Since the Commission does not collect and does not have access to data subjects' personal data, it cannot allow them to access and rectify their data. The Commission will however facilitate the exercise by data subjects of their rights by publishing a privacy statement on the EESSI website indicating how they can exercise their rights. If data subjects contact the Commission regarding access to their data, the latter will invite them to contact the national administration. As concerns the processing operations undertaken by the Commission, data subjects may send an inquiry to the controller by mail or email (contact details are provided on the EESSI website).

**Information to data subjects** shall be provided by the local, regional or national administration where data subjects file a social security benefit claim. In addition, the Commission has adopted a data protection notice which will be posted on the EESSI

---

<sup>10</sup> EC Administrator is required to maintain centralized configuration items in the database.

<sup>11</sup> DS Administrator is a sort of super user, required to start configuration of an empty Directory Service database.

website, which provides information on the processing of personal data in EESSI and on the respective responsibilities of the Member States and of the Commission.

Personal data are **not stored in the EESSI system**, but are kept in repositories by the Access Points of national administrations, under their responsibility. They could also be stored by the Member States' authorities in local databases in cases where national IT systems exist. Personal data are kept for the purposes related to a data subject's claim under the responsibilities of national administrations exchanging them. Data subjects are advised to inquire about the applicable retention periods by contacting the authority to which they filed their claim.

The Commission does not retain any personal data within the infrastructure under its responsibilities. Should the need arise to have short time temporary storage for technical purposes, personal data will anyhow stay encrypted. Messages in transit are stored temporarily for a maximum of 2 days for technical reasons in DIGIT data centre in an encrypted way. They are dispatched as soon as technically possible to the receiving AP.

**Statistics on European exchanges:** Member States are responsible for the collection of statistical data related to data subjects. Article 91 of the basic Regulation provides that statistics shall be collected and organised according to the plan and method defined by the Administrative Commission; these plan and method have not been agreed upon yet and are in working progress. The Commission will collect anonymous data contained in the header/envelope of the messages exchanged between administrations for purpose of producing statistics on European exchanges through EESSI. The following data contained in the header may be used for statistics: SED ID (the unique number identifying a particular SED), SED type, version of the SED, flow ID, flow type, flow version, origin of the SED related information (country, AP, institution where SED originated), destination of the SED information (country, AP, institution of destination), ID of the benefit category, time related information (send data and SED due date if applicable), action type (notification, request, reply, revise, cancel or challenge). The SED ID is processed just as unique record reference number for intermediate processing steps and is dropped in the final statistics that show just aggregated data.

The **security requirements** in EESSI are based on 3 considerations:

- Currently no EU classified data (as defined by Commission Decision 2001/844/EC) are exchanged in EESSI.
- The decision of the EESSI stakeholders is that the protective marking of SED messages is LIMITED HIGH<sup>12</sup>. This refers to a confidentiality level for information systems or information reserved for a limited number of persons on a need to know or need to access principle and whose disclosure to unauthorised persons would cause consequential prejudice to the Commission, other institutions, Member States or other parties, but not to an extent serious enough to merit EU classification.
- This implies that the security requirements for EESSI are "SPECIFIC", which creates the need for additional security requirements based on a limited risk assessment.

A **security risk analysis** was carried out, with the objective to determine what needs to be done, organisationally and technically, based on the proposed architecture of EESSI.

---

<sup>12</sup> Implementing rules for Commission Decision C(2006)3602.

The analysis was undertaken using the CRAMM<sup>13</sup> risk assessment software and focused on confidentiality, integrity and availability. The scope was limited to the infrastructure and communications supporting the core business activities of the EESSI system. This includes the EESSI infrastructure hosted at EC data centre, the national EESSI Access Points and resources supplied by Member States to host the EESSI IT systems and applications. National applications developed by Member States to take part in EESSI and the interconnecting networks (including sTESTA) were out of scope. The deliverable contains a description of the risks, as found by the contractor, on the basis of the specifications of 2009. The end goal is to elaborate customised and adequate countermeasures. The result of the risk analysis is a subset of the more than 3000 detailed countermeasures that are contained in the CRAMM database.

The derived security measures are described in the **security policy**. The security policy sets the standard for implementation and therefore also provides a useful reference to check against. Criteria for risk acceptance and the list of residual risks are however not included in the security plan.

In addition to this security policy, the Commission also developed **several user manuals** for the Coordination Node administrators (i.e., EC administrators at the Commission Data Centre), Directory Services user (i.e. EC administrators of the EESSI directory services) and Reference Implementation user (i.e., WEBIC users/clerks).

The EESSI project organisation and security policy provide for organisational and physical measures both in Member States and at the Commission in order to preserve the security of the data. EESSI security policy covers aspects relating to International Domain central services but also to National Domain applications, which are subject to national security policies. The sTESTA Domain is subject to its own separate security policy.

Amongst the measures set forth in the security policy, the following can be highlighted:

- The origin of SEDs must be authenticated. Further to basic message origin identification (organisation identifier), a secure authentication mechanism shall be present to authenticate the sender. Non-repudiation techniques shall be implemented for messages sent over the network. Confidentiality and non repudiation of data are enforced at the application layer through encryption and signature of data with X.509 certificates issued by a mutually trusted Public Key Authority<sup>14</sup>. At the transport layer, SSL sessions are established between servers to channel HTTP, using X.509 certificates issued by the same PKI. As a result, personal data travel from sending national AP to receiving national AP encrypted and the Commission has no means of accessing it;
- The access control mechanism should be capable of enforcing requirements for segregation of duties and preventing conflicts of interest;
- User identification and authentication information shall be encrypted. Passwords must be stored in such a way that no-one, not even the system administrator, may see them;
- The system should automatically ensure that users follow good security practice in the selection of passwords;

---

<sup>13</sup> Central Computing and Telecommunications Agency (CCTA) Risk Analysis and Management Method.

<sup>14</sup> With respect to the EESSI infrastructure, the Commission appointed the "Réal Casa de la Moneda - Fábrica Nacional de Moneda y Timbre" as the ISA PKI Certification Authority. DG EMPL plays the role of Local Registration Authority for the EESSI closed user group. At national level Member States must choose a national PKI.



- Operator and administrator activity should be monitored to minimise accidental errors and malicious actions. It should not be possible for these activity logs to be modified;
- User access to system data and functions must be strictly controlled. The system should provide protection from unauthorised access by any utility software;
- Both a black box penetration test and a white box test will be performed to ensure that information in the system can not be viewed or accessed by unauthorised persons or insiders using the application for other purposes;
- An audit checking the compliance and implementation of the security policy and procedures should be performed regularly; the frequency of such audits must still be decided by the Administrative Commission. An audit could be foreseen after one or two years of operation of the system;
- Audit logs should be retained for auditability purposes. At the Member States level, the Security Policy describes the events that should be accounted for and provides for a possible minimum retention time of these logs for 3 years. The retention of log files by the Commission is not specifically described in the Security Policy. The Commission informed the EDPS that it will store logs concerning all operations performed by the Coordination Node, which may contain information regarding SEDs such as flow type, flow ID, SED type, SED ID, Origin Access Point, Origin Institution, Destination Access Point, Destination Institution. The retention of technical logs at DIGIT Data Centre is done in accordance with the DIGIT Data Centre Policy, which provides that "log files are retained on disks no more than 10 days";
- Incident management: In the event of any incident or data breach, the EESSI central service desk will get immediately in touch with AP managers and administrators and other ad hoc security fora, in accordance with the "security incident management procedure". A general procedure on incident management is in drafting stage by the Commission; it will be submitted to the Administrative Commission for approval. Furthermore, a **Security Expert Forum (SEF)** has been established to manage EESSI information security, which will be composed of DG EMPL team and representatives from the Member States.. This forum will review periodically the security policy, assess and propose change requests relating to security and follow up possible security incidents drawing lessons learned. The Commission will provide the secretariat for the SEF and for the security response team that will be called upon should a specific "high priority" incident happen.

### **3. Legal analysis**

#### **3.1. Prior checking**

**Applicability of Regulation (EC) No 45/2001 ("the Regulation"):** Insofar as the Commission's activities are concerned, the notified processing falls under the scope of the Regulation and the supervision of the EDPS.<sup>15</sup>

The Commission shall be considered as controller of the processing it carries out in EESSI. As was underlined by the Article 29 Working Party in its Opinion on the concepts

---

<sup>15</sup> For each competent administration, the applicable law is its own national data protection law (in conformity with Directive 95/46/EC) and its activity is supervised by its own national/regional data protection authority.

of controller and processor<sup>16</sup>, the determination of who is/are the data controller(s) should be assessed on a factual basis rather than on a theoretical basis. In view of the information available, the EDPS understands that the Commission contributes to defining the purposes and means used to process personal data in EESSI through its participation, in an advisory capacity, in the Administrative Commission. Furthermore, the Commission is also responsible for the central infrastructure and for ensuring the security of the data exchanged through the common infrastructure. As a result the European Commission shares some responsibilities and duties with respect to EESSI as controller under Regulation (EC) No 45/2001.

The transmission of personal data through an electronic exchange system maintained by the Commission constitutes a processing of personal data; the fact that data are encrypted does not alter the conclusion that the data transmitted are personal data, since they relate to "*an identified or identifiable natural person*" (Article 2 (a) of the Regulation). The data processing is performed by an EU institution in the exercise of activities which fall within the scope of EU law (Article 3 (1) of the Regulation in the light of the Lisbon Treaty). The processing of data is done through automatic means. Therefore, Regulation (EC) No 45/2001 is applicable.

**Grounds for prior checking:** According to Article 27 (1) of the Regulation, "*processing operations likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purpose shall be subject to prior checking by the European Data Protection Supervisor*". Article 27 (2) of the Regulation contains a list of processing operations that are likely to present such risks. The exchanges of information in EESSI include personal data relating to health. The processing of health related data is subject to prior checking by the EDPS pursuant to Article 27(2)(a) of the Regulation.

**Scope of the Opinion:** The recommendations made in this Opinion are addressed to the Commission in respect of its role in designing and operating the EESSI infrastructure insofar that this processing facilitates the exchange of sensitive information between competent administrations and is subject to prior checking on the ground mentioned above.

Although this Opinion does not assess the level of data protection compliance in EESSI at national level, many of the recommendations provided herein can facilitate compliance with data protection rules by users of the system, such as competent administrations in Member States. Therefore, the EDPS recommendations set for the Commission should help ensure a high overall level of data protection within EESSI.

Furthermore, as stated in page 4 above, the EDPS underlines that before any processing is undertaken by the Commission (PMO) in a capacity of competent administration acting as user of the EESSI system for purpose of entitling individuals with their social security rights, the relevant controller should notify him of such processing for prior checking under Article 27(2)(a) of the Regulation.

### **3.2. Lawfulness of the processing**

Article 5 of the Regulation provides criteria for making the processing of personal data lawful. According to Article 5 (a), the processing is lawful if it is "*necessary for the*

---

<sup>16</sup> Opinion 1/2010 of the Article 29 Working Party on the concepts of "controller" and "processor", adopted on 16 February 2010.

*performance of a task carried out in the public interest on the basis of the Treaties...or other legal instruments adopted on the basis thereof*".

The legal basis of the processing carried out by the Commission can be found in the basic Regulation on social security coordination and in Article 4(2) of Implementing Regulation (EC) No 987/2009, which provides that "*The transmission of data between the institutions or the liaison bodies shall be carried out by electronic means either directly or indirectly through the access points under a common secure framework that can guarantee the confidentiality and protection of exchanges of data*".

As to the necessity of the processing, the EDPS notes that the facilitation of the free movement of workers has been a legitimate aim pursued by the EU since the foundation of the European Communities, which involves amongst other things coordinating the social security systems within the EU. Article 48 of the Treaty on the Functioning of the EU sets forth the competences of the EU in the field of social security coordination. Furthermore, the right to social security is a fundamental right protected in Article 34 of the EU Charter of Fundamental Rights. Therefore, the measures developed at EU level to coordinate the social security systems of EU Member States could be considered necessary to guarantee the effective exercise of this fundamental right.

The EDPS welcomes that the processing, which involves special categories of data, is based on a solid legal basis. The EDPS is satisfied that the basic Regulation on social security coordination has been complemented with the Implementing Regulation which provides general implementation measures and that the specific details of the processing are clearly set forth in decisions adopted by the Administration Commission<sup>17</sup>.

### **3.3. Processing of special categories of data**

In the context of EESSI, personal data relating to health and data which may reveal the sexual orientation of individuals (such as civil status) are processed. Processing of personal data concerning health or sex life is prohibited under Article 10 (1) of the Regulation unless grounds can be found in Articles 10(2), 10(3) or 10(4) of the Regulation.

Article 10(4) of the Regulation provides that "*subject to the provision of adequate safeguards, and for reasons of substantial public interest, exemptions (...) may be laid down by the Treaties establishing the European Communities or other legal instruments adopted on the basis thereof or, if necessary, by decision of the EDPS*". The processing undertaken by the Commission is done for purpose of ensuring the implementation of the EU regulations on social security coordination, which will facilitate the effective entitlement of individuals with their social security rights. The processing is therefore done for reasons of substantial public interest, pursuant to the EU regulations on social security coordination. The EDPS considers that the processing of special categories of data by the Commission in the context of operating EESSI infrastructure is justified under Article 10(4) of the Regulation.

However, in view of the limited role of the Commission in the processing of these data the EDPS considers that it is an appropriate measure to require that the Commission only transmits encrypted data so that it does not have access to the content of the sensitive data transiting through EESSI.

---

<sup>17</sup> Referred to in footnote 5.

### 3.4. Data Quality

**Adequacy, relevance and proportionality:** According to Article 4(1)(c) of the Regulation, personal data must be *"adequate, relevant and non excessive in relation to the purposes for which they are collected and/or further processed"*. To ensure the proportionality of the data exchanged, specific provisions of the social security Regulations define the scope of the data that need to be exchanged between competent administrations. In practice, standard forms (Structured Electronic Documents) have been defined by the Administrative Commission for each type of claim, which contain structured mandatory and optional fields to fill in, thereby limiting the amount and types of data to be processed to what is necessary for a particular claim. The processed data appear necessary to evaluate the entitlement of individuals to specific social security benefits. Therefore, the information presented to the EDPS on the data processed appears to meet the requirements of Article 4(1)(c).

**Accuracy:** Article 4(1)(d) of the Regulation provides that personal data must be *"accurate and, where necessary, kept up to date" and that "every reasonable step must be taken to ensure that data which are inaccurate or incomplete are erased or rectified"*. Most of the information will be provided from a competent administration to another. Considering that data will, in most cases, not be collected directly from the data subjects, the rights of access and rectification are important means of ensuring accuracy of the data, which should be available to data subjects (cf. points 3.7).

**Fairness and lawfulness:** Article 4 (1) (a) of the Regulation also provides that personal data must be *"processed fairly and lawfully"*. Lawfulness has already been discussed (cf. point 3.2) and fairness will be dealt with in relation to information provided to data subjects (cf. point 3.8).

### 3.5. Data retention

Article 4 (1) (e) of the Regulation states that personal data must be *"kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed"*.

As concerns the retention of SED messages by the Commission, the EDPS is satisfied with the short retention period of 2 days set forth for purpose of ensuring the transit of messages and with the fact that the data retained are encrypted. The retention of SED messages by the Commission is in line with Article 4(1)(e) of the Regulation.

As concerns the retention of log file information, we understand that the Commission will retain log files of operations performed in the coordination node, which is necessary to monitor and understand how specific technical problems may have developed with a specific flow/message or to verify which events, if any, took place at certain times or intervals. As this is not currently defined in any specific document, the EDPS advises that the categories of log files retained by the Commission in EESSI are properly documented as well as the time limits for their retention. The EDPS emphasizes that, pursuant to Article 37 of the Regulation, the logs collected by the Commission for the operation of the EESSI infrastructure *"should be erased as soon as possible and no later than six months after collection"*. In this view, the EDPS notes that the 10 days retention set forth in DIGIT Data Centre Policy satisfies the requirements of the Regulation.

As concerns retention of data by the Commission for statistical purposes, in accordance with Article 4(1)(e) of the Regulation, the Commission must ensure that the data are

rendered anonymous or, if that is not possible, that the identity of the data subjects is encrypted. In this view, the retention of the SED ID could allow for the indirect identification of the individual whom SED message is about; therefore the data stored for statistical purposes may not be fully anonymous. However, the fact that SED data are encrypted should prevent the Commission from tracing back the data to a specific individual.

### **3.6. Data transfers**

Data are exchanged between designated competent authorities in Member States through the infrastructure maintained by the Commission. Most of these exchanges take place with recipients who apply Directive 95/46/EC and must therefore be analysed under Article 8 of the Regulation, while others take place with recipients who are not subject to Directive 95/46/EC and must therefore be analysed under Article 9 of the Regulation.

The Commission takes part in data transfers to third parties who are subject to Directive 95/46/EC (EU countries and EEA countries which apply Directive 95/46/EC). Article 8 a) of the Regulation provides that data transfers can take place "if the recipient establishes that the data are necessary for the performance of a task carried out in the public interest or subject to the exercise of public authority". In this case, the data transfers clearly fall within the tasks of the competent social security administrations; they therefore respect Article 8 a) of the Regulation.

Furthermore, data transfers may also take place with countries that are not subject to Directive 95/46/EC, namely Switzerland. Such transfers must be analysed in the light of Article 9 of the Regulation. Article 9 notably requires that transfers are made only if an adequate level of protection is ensured in the country of the recipient and the data are transferred solely to allow tasks covered by the competence of the controller. Switzerland benefits from an adequacy decision from the Commission<sup>18</sup> which recognises that it provides an adequate level of data protection. The transfers are made only to social security administrations for purpose of fulfilling their tasks. Therefore Article 9 of the Regulation is respected.

### **3.7. Data subjects rights**

Article 12 of Directive 95/46/EC and the corresponding Articles 13 and 14 of the Regulation establish a right of access upon request by the data subject to his/her data and to have them corrected or deleted under certain circumstances.

The EDPS notes that measures have been taken by the Commission to facilitate the exercise of data subjects' rights in a trans-border context, by designating the administration where the claim was made as the contact point for the exercise of such rights. The Commission, however, will not play a role in granting data subjects' rights in EESSI; in cases of requests, it will only refer the data subject to the contact point.

The EDPS welcomes the solution put forward by the Commission and the designation of a "one stop shop" for exercising data subjects' rights, which should facilitate the effective exercise of rights by data subjects in a trans-border context. The EDPS emphasizes that it shall be the responsibility of that contact point to ensure that data subjects' rights are fully

---

<sup>18</sup> Commission Decision 2000/518/EC of 26.7.2000 - O. J. L 215/1 of 25.8.2000.

enforced. The full exercise of data subjects' rights in a trans-border context will notably require that procedures are put in place between competent administrations for (1) carrying out proper verification of the information that is being challenged, and (2) for notifying all relevant administrations of any rectification/deletion request that has been fulfilled.

### **3.8. Information to data subjects**

Competent administrations are obliged under Articles 10 and 11 of Directive 95/46/EC to provide data subjects with certain information on the processing. Corresponding provisions of the Regulation (Articles 11 and 12) establish similar requirements for the Commission, with respect to the data it processes.

The EDPS notes that in addition to the specific data protection notice that shall be provided by competent authorities at the time when a person files a claim, the Commission has adopted its own data protection notice providing information about the data processing in EESSI, which will be posted on the EESSI website. The data protection notice of the Commission contains all the elements listed in Articles 11 and 12 of the Regulation. The EDPS welcomes such measure, which contributes to making the processing more transparent and provides useful information to data subjects to facilitate the exercise of their data protection rights.

### **3.9. Processing on behalf of the controller**

The EDPS usually considers that a processor is an external organisation to which the EU institution or body outsources certain tasks. However, because of the size of the Commission, the EDPS has accepted the fact that the Commission formalised a system of delegation of the role of the controller within its organisation.

The EDPS notes that the draft standard SLA with DIGIT that was provided to him contains clauses that would satisfy the requirements of Article 23 of the Regulation. However, the EDPS emphasizes that, as stipulated in Article 23(2) of the Regulation, the processing on behalf by a processor "*shall be governed by a contract or legal act binding the processor to the controller*". The EDPS therefore calls on DG EMPL to sign the SLA with DIGIT as soon as possible and in any event before the system fully enters into force.

Furthermore, the EDPS advises that the Commission appropriately documents the respective roles of DIGIT and DG EMPL, G.4, in respect of their access to data and their processing in the different IT systems in EESSI.

### **3.10. Security of data**

The security of health data in a cross-border situation is particularly important. The European Court of Human Rights attached particular weight to the confidentiality of health data: "*Respecting the confidentiality of health data is a vital principle in the legal systems of all the Contracting Parties to the Convention. It is crucial not only to respect the sense of privacy of a patient but also to preserve his or her confidence in the medical profession and in the health services in general*".<sup>19</sup>

---

<sup>19</sup> ECtHR, 17 July 2008, *I v Finland* (appl. no 20511/03), para 38.

The EDPS notes that EESSI stakeholders have agreed on specific measures to preserve the confidentiality of the information flowing through EESSI taking into account the sensitivity of the data.

In particular, the Commission decided to apply to SED messages a protective marking "LIMITED HIGH"<sup>20</sup>, which marking is applied to information systems or information reserved for a limited number of persons on a need to know or need to access principle and whose disclosure to unauthorised persons would cause consequential prejudice to the Commission, other institutions, Member States or other parties. Furthermore, DG EMPL carried out a security risk analysis as one of the deliverables of the EESSI project, which helped identify the countermeasures to be implemented. One of the countermeasures is the EESSI security policy, which is meant to serve as a means of communicating the information security goals, and as a means of providing direction.

The EDPS welcomes the fact that a structured risk assessment has been undertaken, and that a security policy has been established. They provide a useful base for possible future security audits of the EESSI system.

The EDPS however notes that the security policy is quite detailed in some areas and less detailed in others. The EDPS advises that the Commission complements the security policy with more detail in those areas where needed.

Furthermore, the EDPS did not receive any information on any concrete planning for audits of the system. As put forward in the security policy, an audit checking the compliance and implementation of the security policy and procedures should<sup>21</sup> be performed regularly, but the frequency of such audits must still be decided by the Administrative Commission. The EDPS recognises that, to make the link from theory to practice, it would be highly useful to carry out one or more security audits, at the very beginning of the system operation, after important changes in the system, or periodically. The audit would provide insight into how much of the security policy has actually been implemented and where more work needs to be done. As such, it would make for a valuable management tool. The EDPS therefore recommends that the Commission establishes a workable audit plan and conducts one or more security audits of the system.

#### **4. Conclusions**

The EDPS considers that there is no violation of Regulation (EC) No 45/2001 provided that the Commission fully takes into consideration the above considerations before the EESSI system enters into force. In particular, the Commission should:

- only transmit encrypted data, so that it does not have access to the content of the sensitive data transiting through EESSI;
- appropriately document the categories of log files it will retain and the time limits for their retention;
- help ensure that data subjects can fully enforce their rights at the relevant contact point in the Member State. This will notably require that procedures are put in place between competent administrations to designate a central point of contact

<sup>20</sup> Implementing rules for Commission Decision C(2006) 3602 of 16/8/2006.

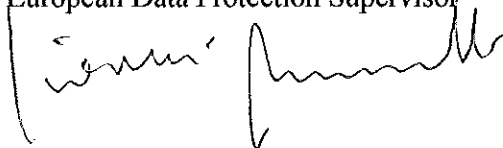
<sup>21</sup> In the security policy document, use of "should" implies a strong recommendation (as opposed to an essential and mandatory security control, and to a recommendation).

for the data subject, to verify the information that is being challenged and to notify all relevant administrations of any rectification/deletion request that has been fulfilled;

- enter into a legally binding SLA with DIGIT which contains appropriate clauses satisfying the requirements of Article 23 of the Regulation before the system fully enters into force;
- appropriately document the respective roles of DIGIT and DG EMPL, G.4, in respect of their access to data and their processing in the different IT systems in EESSI;
- complement the security policy with detailed provisions, especially in those areas where the policy remains high level;
- establish a workable audit plan and conduct one or more security audits of the system;
- notify the EDPS of any substantial change to the design of the system which would impact the level of data protection in EESSI.

Done at Brussels, on 28 July 2011

Giovanni BUTTARELLI  
Assistant European Data Protection Supervisor

A handwritten signature in black ink, appearing to read 'Giovanni Buttarelli', written over a horizontal line.