DPO-3326.1 - EMPL : EESSI - Electronic Exchange of Social Security Information

General information

Creation : 13/12/2010

Last updated : 19/03/2012

Registration : 09/12/2011

Status : Register

Deleted : No

DG.Unit : EMPL.B.4

Controller : MORIN Jackie

Delegate :

DPC : CORTELLESE Alberto

Keywords :

Corporate : No

Language : English

Model : No Model

EDPS opinion (prior check) : No

Target Population : Citizens

DPC Notes :

Processing

1 . Name of the processing

EESSI - Electronic Exchange of Social Security Information

2 . Description

The system allows the exchange of personal social security information among competent national administrations.
National Access Points (APs), hosted in participating countries, are connected to local sTESTA Local Domain Connection Points (LDCPs) and among them in a star topology by sTESTA infrastructure. The centre of the star is called Coordination Node and is hosted at the EU Commission Data Centre. The Configuration Node's role is just to dispatch info and collect statistics (no personal data collected).
APs are featured with a web application allowing national administration clerks to enter data to be exchanged with other national administrations. APs also feature a business-to-business interface allowing the interconnection of national systems with EESSI.

Unit "Coordination of social security schemes, free movement of workers" of DG Employment, social Affairs and Equal Opportunities plays the role of project manager, system developer, supports EESSI central infrastructure and part of the peripheral infrastructure, and coordinates all stakeholders. Business and data owners are the participating countries (European Economic Area and Switzerland).

The EESSI project "steering committee" is represented by the Administrative Commission for Social Security Coordination and other committees stemming from the legal basis (see "Legal basis/lawfulness" section), who are then the main controllers.

Further info can be found in here: <style isUnderline="true" forecolor="#0000FF">http://ec.europa.eu/social/main.jsp?langId=en&catId=869</style>

Some processing operations performed by EESSI system are subject to prior checking by the EDPS, pursuant to paragraph 2, points a) and d) of art. 27 of Reg.45/2001 (hereinafter called "the Regulation").

For prior checking outcome, see EDPS Opinion 2011-0016 of 28 July 2011.

No automated decision is taken excluding data subjects from rights.

3 . Processors
N.A.

4 . Automated / Manual operations
See "Description" section.

5 . Storage
Personal data of migrant workers are stored in repositories by the Access Points of national administrations, under their responsibility. They could also be stored elsewhere in case of existence of national IT systems having the same business purposes and interacting with EESSI through a "business to business" interface.
Messages in transit are stored temporarily (planned maximum storage time is two days) for technical reasons in DIGIT Data Centre in an encrypted way (see "Technical and organisational measures" section). They are dispatched as soon as technically possible to the receiving AP.

Contact details of the MMI users and business contact details of contact persons in national administrations are stored in servers hosted at the DIGIT DC under Commission's responsibility.

6 . Comments
-

Purpose & legal basis

7 . Purposes
The aim of the EESSI (Electronic Exchange of Social Security Information) project is to strengthen the protection of citizens' rights by computerising the exchange of social security information on migrant workers between competent national institutions in the field of social security in the application of Regulations 883/2004 and 987/2009 on social security coordination. IT-based exchanges of migrant workers' social security related information will:

• facilitate and speed up the decision-making for the calculation and payment of social security benefits;
• allow a more efficient verification of data;
• provide a more flexible and user-friendly interface between different systems;
• provide an accurate collection of statistical data on European exchanges.

8 . Legal basis and Lawfulness
Regulation (EC) No 883/2004 of the European Parliament and of the Council of 29 April 2004 on the coordination of social security systems (Text with relevance for the EEA and for Switzerland), as amended by Regulation 988/2009, recital 40, articles 77, 78.

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 (Text with relevance for the EEA and for Switzerland),

- recitals 3, 4, articles 1, 2, 4, 88, 95 provide the basis for putting in place the EESSI system to implement the obligation for an electronic data exchange between the national institutions.

- the specific provisions in Reg. 883/2004 and 987/2007 that provide specific rules on the coordination of the national social security schemes within each of the different social security sectors (sickness, family benefits, unemployment benefits, pensions, occupational diseases, etc), define the scope of the data that need to be exchanged between the national institutions in the application of these specific provisions. These specific provisions provide a solid basis to ensure that the proportionality principle in the collection of personal data is

respected.

Council Regulation (EC) No 859/2003 of 14 May 2003 extending the provisions of Regulation (EEC) No 1408/71 and Regulation (EEC) No 574/72 to nationals of third countries who are not already covered by those provisions solely on the ground of their nationality, and its successor.

Processing is lawful pursuant to art. 5, point a) of the Regulation. Even though some data categories are within those listed in art. 10 paragraph 1 of the Regulation, this provision does not apply pursuant to art. 10, paragraph 2, point b).
As stated in the "Description" section, prior checking by EDPS is applicable.

Data subjects and Data Fields

9 . Data subjects

Workers, and their family members, having worked in more than one of the participating countries and claiming for social security benefits. The new Regulations on social security (i.e. Regulation (EC) No 883/2004 and Regulation (EC) No 987/2009), which entered into force on 1 May 2010, also coordinate the social security rights of non-active persons that have links with more than one of the participating countries.

For access control purposes: users allowed to upload, modify and download EESSI Directory Services data (hereinafter called "MMI users"), currently public non-personal data.

10 . Data fields / Category

1) Data categories needed for (non) granting social security benefits (hereinafter SED data: Structured Electronic Documents). In particular:

Name, sex, address, birth date and place, residence info, 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.), info on patient's health (including e.g. medical exams/treatments) and accidents, info on benefits enjoyed, financial info (including bank account, fiscal identification and trade register numbers, income), employment status and employment record (including reason for termination).

As regards the information on the deceased members, this data can be relevant for the entitlement to a social security benefit of a person that has a link with the deceased, i.e. for the purpose of receiving a survivor's pension. This information shall be kept until the moment that the right to the benefit linked to the deceased member ceases to exist, e.g. because the entitled person has also died.

Some categories (health, family civil status – which can disclose possible sexual orientation as an indirect info) fall under art.10. See also "Legal basis/lawfulness" section. The sexual orientation can be derived from civil status of a person (e.g. civil partnership, which in certain countries is open for couples of the same sex).

2) Contact details of MMI users for access control purposes (see "Data subjects" section).

3) Business contact details of contact persons of national administrations: name, surname and business addresses.

Rights of Data Subject

11 . Mandatory Information

See attachments.

List of attachments

- art15-EESSI notification.doc
- EESSI website - Personal data protection in EESSI.doc

12 . Procedure to grant rights

See "Mandatory information" section.
Data subjects will contact the competent administration where they applied for their claim of social security benefits.
If a data subject contacts the Commission, the latter will invite the data subject to contact the national administration. In addition, the Commission will invite the data subject to consult all the public documentation on the project, including personal data protection aspects, published on EESSI web site (see also notification on section "Mandatory information").

13 . Retention

Personal data are kept for business purposes under the responsibilities of countries exchanging them (see "Storage"section). 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 (planned maximum storage time is two days), personal data will anyhow stay encrypted.

14 . Time limit

N/A. This applies to countries.

15 . Historical purposes

-

Recipients

16 . Recipients

1) SED data: clerks of national administrations competent in the relevant specific sector of social security.

2) MMI users: DG EMPL staff supporting EESSI.

3) Business contact details: public.

17 . Transfer out of UE/EEA

-

Security measures

18 . Technical and organizational measures

Technical measures

A system security policy following up a risk assessment exercise (documented) exists for the system. Some outstanding measures follow hereinafter.
Relevance and proportionality of personal data are ensured by specific structured messages (SED) to be exchanged according to a business protocol serving business needs. Both message structure and protocol are approved by relevant steering committees and working groups thereof, which consist of representatives from the Member States.
Access control to the web application used to input/output messages is enforced through a UserID/Password combination with strong password policy. Confidentiality and encryption of data exchanged are enforced at the application layer through signature and encryption of data with X.509 certificates issued by a mutually trusted

Public Key Authority. At the transport layer, SSL sessions are established between servers to channel HTTP. Appropriate logging for auditability is provided, too.
Please see also notification N°1 (infrastructure under DIGIT responsibility). Outstanding measures: while flowing through sTesta infrastructure (under DIGIT responsibility) network layer protection in enforced though IPsec.
Organisational measures

The EESSI project organisation and Security Policy provide for organisational measures both in countries and at the Commission. As regards Commission's responsibilities, please see notification n.1 (infrastructure under DIGIT responsibility).
A hosting proposal was agreed between DG EMPL and DIGIT for the operation of central EESSI infrastructure hosted at the Commission Data Centre. Furthermore, central EESSI service desk is operated by DG EMPL staff and relevant working procedures are documented.

In case of risk of a breach of security the EESSI central service desk will get immediately in touch with AP managers and administrators.

19 . Complementary information

1) On data processors.
Central components of EESSI (those managed by DG EMPL) are hosted by DIGIT Data Centre through a hosting contract.
2) EESSI overview presentation in attachment

Further technical documents on request.

List of attachments

- EESSI overview.pdf
- EESSI overview.zip