EUROPEAN COMMISSION
Employment, Social Affairs and Inclusion DG

Employment and Social Legislation, Social Dialogue
Free Movement of Workers, Coordination of Social Security Schemes

Brussels,
EMPL/B/4/SK/sc (2011)

Subject: **Follow up on EDPS' final Opinion on the notification for "prior checking" on the Electronic Exchange of Social Security Information system ("EESSI").**

1. INTRODUCTION

On 28 July 2011 the European Data Protection Supervisor notified the Commission of his Opinion (hereafter "the 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"). We would like to thank the EDPS for his Opinion and his contribution towards a lawful system.

The Opinion concluded that there is no violation of Regulation (EC) No 45/2001 provided that the Commission fully takes into account some considerations elaborated in the text and in particular specific recommendations before the EESSI system enters into force.

The EDPS invited the Commission to inform him within three months of the measures taken based on those recommendations.

Section 3 reports how the Commission has addressed such recommendations so far.

2. LATEST DEVELOPMENTS IN EESSI PROJECT

2.1. Extension of the transitional period for the implementation of the EESSI.

The European Commission would also like to take this opportunity to inform the EDPS about some latest development in the EESSI project.

According to Article 95(1), first subparagraph, of Regulation (EC) No 987/2009, the transitional period for the implementation of the EESSI system in the Member States is 24 months, starting from 1 May 2010, when this Regulation has become applicable. According to these transitional arrangements, EESSI would thus be operational at the latest by 30 April 2012.

On the basis of an overall assessment of the planning at both central Community level and Member States' level, it has been concluded recently that this is not

feasible. The implementation has encountered certain delays, due to the complexity of this large scale integration IT project, both IT and business wise. Therefore, in its 328th meeting, which took place on 18 and 19 October 2011, the Administrative Commission for the coordination of social security systems has decided to extend the transitional period until 30 April 2014. Member States can start their exchanges earlier during this period. It is foreseen that the first Member States will be ready for electronic exchange of their data beginning 2013.

2.2. Meetings of other governance bodies and expert groups.

During the 50th meeting of the Technical Commission for the coordination of social security systems (hereinafter "TC"), which took place on 5 and 6 October 2011, the Opinion was presented and the recommendation in section 3.3 below was particularly highlighted because of their role in implementing it.

This year also the Security Expert Forum (hereinafter "SEF") has been established by EESSI Technical Commission to manage EESSI security. The SEF met on 11 October 2011. Among others, the EDPS Opinion was presented and possible actions to enforce recommendation in section 3.6 below were discussed and decided.

3. FOLLOW UP OF RECOMMENDATIONS

3.1. The Commission should only transmit encrypted data, so that it does not have access to the content of the sensitive data transiting through EESSI.

All personal data travel encrypted in the SED message payloads when transiting through the Commission infrastructure. SED decryption is possible only through cryptographic keys in possession of the manager of the addressee Access Point. Further encryption then exists for most of the subsystems under Commission responsibilities at the transport and network layer (HTTP over SSL, IPSec).

For references to system documentation, see Annex I.

3.2. The Commission should appropriately document the categories of log files it will retain and the time limits for their retention.

A document has been created documenting the log files retained by the Commission. You can find information on those logs in Annex II.

3.3. The Commission should 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 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.

In the 50th meeting of the TC, the European Commission has reminded the Member States' representatives of their obligations under Directive 95/46 EC to ensure that data subjects can fully enforce their rights at the relevant contact point in the Member State. To that end, it has been agreed, that the Member States will provide the Secretariat with information on the contact point(s)

that are established or to be set-up to that end in their country. This list, which will be prepared in the following months, will also be made available on the Commission's website.

3.4. The Commission should 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.

DG EMPL and DIGIT are currently active establishing a generic SLA between DG EMPL and DIGIT covering all IT projects managed by DG EMPL and hosted in DIGIT. It will of course contain specific needs arisen by the various systems, including EESSI. This SLA is planned to be signed by 31 December 2011.

This SLA is built upon DIGIT SLA template. The latter stipulates what the service provider will do on behalf of the controller, defining responsibilities, also as regards personal data protection issues.

3.5. The Commission should 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.

Respective roles of DIGIT and EMPL in EESSI system deployed in DIGIT Data Centre are clearly regulated by the forthcoming SLA (see section 3.4). DIGIT staff has in any case no access to EESSI operational data. They will have access to technical logs, not containing personal data. DG EMPL has access to some operational data, of which none can be classified as personal data pursuant to the meaning of Reg. 45/2001.

3.6. The Commission should complement the security policy with detailed provisions, especially in those areas where the policy remains high level.

We take note that the EDPS did not specify in which areas the policy remains high.

The EESSI Project Team in DG EMPL started a preliminary analysis, which formed the basis of a discussion point at the 1st SEF meeting. In the "Report and recommendations of the 1st meeting of the Security Experts Forum" it is reported that "...the SEF agreed that it will undertake a review of the EESSI Security Policy ... with a view to further improve or detail this document...". According to the work plan, the revised Security Policy will be submitted to the EESSI Steering Committee by end April 2012. Further to the improvement of the Security Policy document itself the current work plan provides for an Incident Management and an Anti Malware standard to be drafted.

3.7. The Commission should establish a workable audit plan and conduct one or more security audits of the system.

The audit plan will be established in the context of the review of the security policy document (see section 3.6). In any case the Commission will provide for an audit of that part of the system under its responsibility no later than one year after the end of the transitional period.

3.8. The Commission should notify the EDPS of any substantial change to the design of the system which would impact the level of data protection in EESSI.

No substantial changes in the design so far. Major project management changes have been reported above in section 2.

Yours sincerely,

Jackie MORIN
Head of Unit