Opinion on a notification for Prior Checking received from the Data Protection Officer of the European Parliament concerning the "Security Support System"

Brussels, 29 September 2009 (Case 2009-0225)

1. Proceedings

On 1 April 2009, the European Data Protection Supervisor (EDPS) sent a letter to the Data Protection Officer of the European Parliament (EP) on a consultation[1] about the need to prior check the present processing activity. The answer of the EDPS considered that the case had to be subject to prior check, stating that the date of the notification to be registered was the date of the mentioned letter.

On 6 April and 19 August 2009, the EDPS requested additional information from the EP. The responses were received on 22 June and 28 August 2009, respectively. On 11 September the draft Opinion was sent to the DPO for comments and the answer was received on 24 September 2009.

2. Facts

- Purpose of processing

The collection of data in the Security Support System has the purpose to provide support to missions outside the three places of work of the EP in case of medical emergencies. The information is provided by the data subject on a voluntary basis. Data will only be used in emergency situations and only given to local health staff if needed. The data subject is not obliged to provide any information.

- Data subjects

The data subjects concerned are Members of the European Parliament (MEPs) and staff on delegations.

- Categories of data

The categories of personal data are the following:

- medical information (in case of emergency if participant is found unconscious, e.g. medication needed, allergy information, rare blood group)
- contact details of emergency contact (next-of-kin).

[1] The consultation was submitted by the DPO on 19 February 2009 (case 2009-0158).

- Information to the data subjects

The following information is provided to the data subject(s):

- the identity of the controller;
- the purposes of the processing;
- the categories of recipients of the data;
- the fact that provision of information is voluntary ("You are not obliged to provide any information. However, it may imperil your health or result in difficulty in contacting your next of kin if relevant information is not provided")
- the existence of the right of access and the right of rectification;
- the legal basis of the processing (consent);
- the time limits for storing the data;
- the right to have recourse at any time to the European Data Protection Supervisor.

- Procedures to grant rights of data subjects

In general: implementing rules relating to Regulation (EC) No 45/2001 contained in the Bureau decision of 22 June 2005 provide for the right of data subjects in Articles 8 - 13. Specifically for this operation: the collection is voluntary and data subjects are informed of their rights by a statement on the form. Furthermore, instructions have been given to DG EXPO staff in this regard.

- Type of processing (automated and/or manual)

The processing activity conducted is manual. Information on medical data and emergency contact/next of kin shall be collected and forwarded to the security officer as paper copy only. Any information on medical data and next of kin received in electronic form is deleted immediately from the E-Mail-drive and is not stored on any other drives, in accordance with instructions to staff.

- Storage media

The storage media used is paper.

- Recipient(s) of the Processing

A possible transfer to local health care services in case of emergency may take place.

- Retention policy

Destruction on safe return of delegation is foreseen.[2]

- Time limit to block/erase data on justified legitimate request from the data subjects

Destruction on safe return of delegation is foreseen.

- Security and organisational measures

[2] This procedure is foreseen in the internal document of DG EXPO "Interim support system to outgoing delegations. Tools, tasks and procedures", updated 18/05/2009.

(...)

3. Legal aspects

3.1. Prior checking

***Applicability of Regulation (EC) No 45/2001*:** The collection of data in the Security Support System constitutes processing of personal data ("*any information relating to an identified or identifiable natural person*" - Article 2 (a) of the Regulation). The data processing is performed on behalf of a Community body, in this case the European Parliament, in the exercise of activities which fall within the scope of Community law (Article 3 (1) of the Regulation). The processing of the data is done manually and form part of a filing system. 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. This list includes Article 27 (2) (a): "*processing of data relating to health and to suspected offences, offences, criminal convictions or security measures"*. The processing in question includes data relating to health.

Deadlines: The notification of the DPO was registered on 1 of April 2009. According to Article 27 (4) of the Regulation, the EDPS opinion must be delivered within a period of two months. The procedure was suspended for a total of 90 days plus the month of August (121 days) to require additional information and to allow for comments from the data controller. Consequently, the present opinion must be delivered no later than on 29 September.

3.2. Lawfulness of the processing

Article 5 of Regulation (EC) No 45/2001 provides criteria for making processing of personal data lawful. One of the criteria provided in Article 5 (d) is that the *"data subject has unambiguously given his or her consent"*.

Article 2(h) of the Regulation defines "data subject's consent" as follows: *"any freely given specific and informed indication of his or her wishes by which the data subject signifies his or her agreement to personal data relating to him or her being processed"*.

It has to be noted that in the context of employment, the use of "consent" as a legal basis presents some restrictions.[3] Nevertheless, in the case under analysis, the data subject is free to provide or not the categories of data above mentioned. He or she is informed about this freedom, in the light of Articles 2(h) and 5(a) of the Regulation and also about the possible consequences of not providing the information.

3.3. Processing of Special Categories of Data

[3] Article 29 Working Party, Opinion 8/2001 on the processing of personal data in the employment context, Adopted on 13 September 2001, 5062/01/EN/Final WP 48, available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2001/wp48en.pdf , *"The Article 29 Working Party takes the view that where consent is required from a worker, and there is a real or potential relevant prejudice that arises from not consenting, the consent is not valid in terms of satisfying either Article 7 or Article 8 as it is not freely given. If it is not possible for the worker to refuse it is not consent. Consent must at all times be freely given. Thus a worker must be able to withdraw consent without prejudice."*

Article 10.1 of Regulation (EC) No 45/2001 establishes that *"the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and of data concerning health or sex life, are prohibited"*. The prohibition is lifted if grounds can be found in Articles 10(2) and 10(3) of the Regulation. Among others, such grounds include the consent of the data subject ex Article 10(2)(a). The EDPS considers that the processing activity analysed can take place under this rule.

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"*. The information presented to the EDPS on the data processed appears to meet those requirements.

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"*.

To the extent that the data subjects provide the information themselves, the procedure itself appears to ensure that the data are accurate and kept up to date as much of the personal data supplied are provided by the data subject. In this regard, as further developed below, it is important that appropriate security measures ensure the integrity of the data (see Section 3.9). It is also important for the data subject to be able to exercise the right of access and rectification insofar as it enables individuals to control whether the data held about them is accurate (see Section 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"*.

According to the information received, the EP keeps the data for the duration of the mission. Then, the data is destroyed after the safe return of the delegation. The exact length of the period will vary depending on the duration of the mission. The EDPS considers this policy as being in accordance with Article 4(1)(e).

3.6. Transfer of data

In the case under analysis, a possible transfer to health care services of the country where the mission is conducted may take place. This processing may involve a transfer to a recipient subject to Directive 95/46/EC, in case the health care service is located in a country of the EEA. The processing may also involve a transfer to a third country. In the first case, account should be taken to Article 8, and in the second, of Article 9 of the Regulation.

Article 8 foresees that: *"[w]ithout prejudice to Articles 4, 5, 6 and 10, personal data shall only be transferred to recipients subject to the national law adopted for the implementation of Directive 95/46/EC, (...)(b) if the recipient establishes the necessity of having the data transferred and if there is no reason to assume that the data subject's legitimate interests might be prejudiced"*. In the present case, the necessity of the transfer has to be proven *per se*, since it can only take place in case of medical emergency. Furthermore, since the data subject has given his or her consent to the processing, there would be no reason to assume, in principle, that his or her legitimate interests might be prejudiced.

In line with Article 9.1 of the Regulation, *"personal data shall only be transferred to recipients, other than Community institutions and bodies, which are not subject to national law adopted pursuant to Directive 95/46/EC, if an adequate level of protection is ensured in the country of the recipient or within the recipient international organisation and the data are transferred solely to allow tasks covered by the competence of the controller to be carried out"*.

Article 9.6 stipulates that: *"[b]y way of derogation from paragraphs 1 and 2, the Community institution or body may transfer personal data if: (a) the data subject has given his or her consent unambiguously to the proposed transfer; or (...)(e) the transfer is necessary in order to protect the vital interests of the data subject; (...)"*.

The processing activity being analysed would, in principle, fall under these derogations.

3.7. Right of access and rectification

The following provisions are applicable in the present case:

(i) Article 13 of Regulation (EC) No 45/2001 that provides a right of access to personal data being processed; *(ii)* Article 14 of Regulation 45/2001 that provides a right to rectification without delay of inaccurate or incomplete data;

The notification refers to the general rights of the data subjects according to the Bureau decision of 22 June 2005 (Articles 8-13). The EDPS considers that the rights of access and rectification are therefore recognized.

3.8. Information to the person concerned

Pursuant to Articles 11 and 12 of Regulation (EC) No 45/2001, those who collect personal data are required to inform individuals that their data are being collected and processed unless the data subject already has this information. Individuals are further entitled to be informed of, inter alia, the purposes of the processing, the recipients of the data and the specific rights that individuals, as data subjects, are entitled to.

As described under point 2, data subjects are informed accordingly in the present case.

3.9. Security measures

According to Article 22 of Regulation (EC) N° 45/2001, *"the controller shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks presented by the processing and the nature of the personal data to be protected*". These security measures must *"in particular prevent any unauthorised disclosure or access, accidental or unlawful destruction or accidental loss, or alteration, and to prevent all other unlawful forms of processing".*

The EDPS has no reason to believe that these and other additional implemented measures are no adequate in light of Article 22 of the Regulation.

4. Conclusion:

There is no reason to believe that there is a breach of the provisions of Regulation (EC) No 45/2001.

Done at Brussels, 29 September 2009

(signed)

Giovanni BUTTARELLI
Assistant European Data Protection Supervisor