**Opinion on a notification for Prior Checking received from the Data Protection Officer of the European Parliament concerning the "Safe Mission Data" system**

Brussels, 24 May 2012 (Case 2012-0105)

## 1. Proceedings

On 31 January 2012, the European Data Protection Supervisor (**EDPS**) received a notification for prior checking relating to the processing of personal data regarding "Safe Mission Data" from the Data Protection Officer (**DPO**) of the European Parliament (**EP**).
Questions were raised on 2, 16 and 24 February 2012 to which the controller replied on 16 and 23 February 2012, successively expanding the scope of the initial notification to include the use of another database in the context of the data processing operation. The DPO replied to the questions raised on 24 February 2012 on 20 March 2012. The draft Opinion was sent to the DPO for comments on 11 April 2012. The EDPS received a reply on 19 April 2012 and further clarifications on 7 May 2012.

## 2. Facts

The collection of data, including in particular health data, in the "Safe Mission Data" system (SMD) has the **purpose** of providing support to delegations outside the three places of work of the EP by contributing to a rapid and effective reaction in the case of any emergency situation. A database[1] will contain all participants' personal and travel data; for each separate mission, two envelopes containing hard copies of this data will be prepared to provide two responsible officials with precise, accurate, reliable and relevant data in order to take all the appropriate security decisions should an emergency situation arise. The data is partially recovered from a database ("CODICT", which contains staff data previously provided by the data subjects on a voluntary basis) as well as the travel agency for mission data and, for the other part, provided by the data subjects on a voluntary basis by means of a collection form.

**Data subjects** are Members of the European Parliament (MEPs) forming part of a traveling delegation, including support staff (EP officials, interpreters, political advisors). The data base will be voluntary for other persons that might be present on the place of a delegation, e.g. MEP's assistants.

The **legal basis** are the Decision of the Conference of Presidents of 10/3/2011 on implementing provisions governing the work of delegations, in particular its Annex IV: "Protocol on emergencies arising during official travel activities outside the three places of work" as well as the Bureau Decision on "Travel by Committee Delegations outside the three places of work of the European Parliament" of 2/10/2000 as amended by Bureau Decisions of 14/11/2011 and 12/03/2012.

[1] Replacing a paper-based system which fulfilled the same purpose and had previously been prior checked (case 2009-0225, EDPS Opinion of 29 September 2009)

The **categories of personal data** processed are twofold: data which are by its nature relevant for every mission and data relevant only to the specific mission.

1. The following data are transferred from a database named "CODICT"[2] (which has not been notified to the EDPS and is not covered by the present Opinion):
   - General staff information, such as first name, last name, address (reference data such as town codes, country codes etc.) or unit / political group;
   - Passport number for MEPs, where available in "CODICT".
2. Travel data ("missions"), such as flight numbers, hotels, dates of travel and stay, are obtained from the travel agency based on the information previously provided by the data subject in the mission order or from the data subject himself/herself.
3. Additionally, by means of a collection form, each data subject is asked to provide the following complementary categories of personal data:
   1. health data and specific requests regarding any special conditions required due to the particular characteristics of an individual[3];
   2. next of kin/contact person, address, telephone numbers;
   3. date of birth, nationality, address, gender, telephone numbers, number of passport or identity card with a copy;
   4. "proof of life" question and answer for use in kidnap situations.

The following **information** is provided to the data subjects in the collection form:
- the identity of the controller;
- the purposes of the processing[4];
- the categories of recipients of the data;
- the fact that provision of information is voluntary[5];
- the existence of the right of access and the right of rectification;
- the right to have recourse at any time to the European Data Protection Supervisor.

**Recipients** of this data include:

- Staff of the Resource Management Directorate. However, they will not have access to health data. Access to this information is given only to the medical service, which prints it and seals it in envelopes, two for each mission.
- DG PRES Directorate for Security will have permanent access to SMD to enable them to solve any emergency situation, but without access to health data.
- A sealed envelope containing health information will be opened only by a care giver in the event of a medical emergency; in this context, data may be disclosed to local care givers (such as medical professionals) in third countries.
- Under certain circumstances such as a terrorist attack, where a rapid and effective reaction in the case of an emergency situation is required, the above data may be disclosed to the Joint Situation Centre of the European External Action Service and/or embassies or consulates of Member States.

The **rights of data subjects** are generally contained in Articles 8 - 13 of the Bureau Decision of 22 June 2005 stipulating the Implementing Rules for Regulation (EC) No 45/2001[6].

[2] Notified to the DPO of the EP under Article 25 of the Regulation as No. 101, see http://www.europarl.europa.eu/data-protect/dispatch.do.
[3] E.g. dietary requirements (e.g. food allergy), accommodation requirements (e.g. wheelchair use), information for on-the-spot medical care (e.g. blood group) or restrictions on medical treatment to be applied (e.g. in respect of religious beliefs).
[4] "*In an emergency, you may be unconscious or otherwise unable to inform your care providers about your medical history. This form is meant to help you get the care you need in a life-threatening situation. This form will be kept sealed and will only be disclosed to caregivers in case of emergency*".
[5] "*You are not obliged to provide any information. However, it may endanger your health or result in difficulty in contacting your contact person if the relevant information is not provided*".
[6] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2005:308:0001:01:EN:HTML.

**Retention policy**: Data which is by its nature relevant for every mission (see above "categories of personal data", sub-points 1 and 3) will be erased at the end of the legislature for MEPs and on completion of service for EP staff; travel data relevant only to the specific mission will be deleted from the database upon return from that particular mission. All paper copies (contained in two envelopes, one kept by the Security DG EXPO Officer and the other one given to the responsible administrator accompanying the delegation) are destroyed after return from the mission.

[...]

## 3. Legal aspects

### 3.1. Prior checking

***Applicability of Regulation (EC) No 45/2001*** (the Regulation): The collection of data in the SMD system constitutes processing of personal data ("*any information relating to an identified or identifiable natural person*" - Article 2(a) of the Regulation)[7]. The data processing is performed 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 activity is both automated and manual, in the latter case forming part of a filing system.
Therefore, the Regulation 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)) 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 received on 31 January 2012 and registered on 1 February 2012. 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 72 days to request additional information and to allow for comments from the data controller. Consequently, the present opinion must be delivered no later than 11 June 2012.

### 3.2. Lawfulness of the processing

Article 5 of the Regulation provides criteria for making processing of personal data lawful.

a) Pursuant to Article 5(a), the processing is lawful if it is "necessary for performance of a task carried out in the public interest on the basis of the Treaties establishing the European Communities or other legal instruments adopted on the basis thereof (...)". This includes "the processing necessary for the management and functioning of those institutions and bodies" (recital 27). It follows that the first issue under Article 5(a) is to determine whether there is a specific legal basis for the processing and the second issue is to verify whether the processing in question is necessary for the performance of a task carried out in the public interest.

The rules governing the processing operation under analysis are found in all legal provisions indicated in the facts, which serve as legal basis for establishing the relevant lists of the data subjects concerned. As concerns necessity under Article 5(a), the processing of data

[7] According to the notification, the "proof of life" question arguably does not constitute personal data in the sense of Article 2 of the Regulation, "*as the information does not need to be accurate*". However, the purpose of including a "proof of life" question according to the notification consists of enabling "*authentification of identity in the case of kidnap or hostage situations*", thus information (independent of its accuracy) related to a natural person (chosen by this individual) to make him/her indirectly identifiable in such situations. At any rate, such "proof of life" question may contain personal data.

*transferred* from the **"CODICT" database as well as the travel data** obtained from the travel agency is considered as "necessary for the performance of a task carried out in the public interest", in view of providing support to delegations outside the three places of work of the EP by contributing to a rapid and effective reaction in the case of any emergency situation.

However, in order to ensure lawfulness under Article 5 of the Regulation with regard to data stemming from the **"CODICT" database and the travel agency**, the EDPS recommends ensuring that data subjects freely give their unambiguous consent *at the time of collection* of data for "CODICT" and the mission order to using that data also in the context of the SMD.

b) **Article 5(d)** permits processing where the *"data subject has unambiguously given his or her consent"*. Article 2(h) of the Regulation defines "data subject's consent" as *"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 "*For consent to be valid, it must be freely given. ...Data processing operations in the employment environment where there is an element of subordination...may require careful assessment of whether individuals are free to consent*"[8].

In the case at hand, nothing indicates any element of constraint on a data subject to give consent in the context of filling in the **collection form**[9]; rather, he/she is explicitly informed in the form itself[10] that there is no obligation to provide any information and also about the possible consequences of not providing the information. The consent given by the data subjects should therefore be considered as "unambiguously" and "freely given" in the sense of Articles 5(d) and 2(h) of the Regulation. Insofar, the processing of personal data can be considered lawful.

### 3.3. Processing of Special Categories of Data

Article 10(1) of the Regulation 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"*. In the case at hand, SMD will by its very purpose reveal health data. The prohibition of Article 10(1) of the Regulation 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 under Article 10(2)(a). In the light of the considerations under Section 3.2 above, the EDPS considers that the conditions of this provision are met as regards health data processed in the context of SMD; the prohibition under Article 10(1) of the Regulation consequently does not apply insofar.

### 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"*.

[8] See Opinion 15/2011 of the Article 29 Data Protection Working Group on the definition of consent (WP 187 of 13 July 2011), p. 34.

[9] See Article 8, third sub-point of Annex IV ("Protocol on emergencies arising during official travel activities outside the three places of work") of the Decision of the Conference of Presidents of 10/3/2011 on implementing provisions governing the work of delegations referring to "...a *confidential data sheet...containing all relevant particulars which may be required in the event of a medical emergency or hospitalisation*..."

[10] Entitled "Voluntary Emergency Medical Information" (emphasis added), noting that "*You are not obliged to provide any information. However, it may endanger your health or result in difficulty in contacting your contact person if the relevant information is not provided*..."

To the extent that the data subjects provide the information themselves (for use in "CODICT", by providing the information contained in the mission order as well as by means of the collection form), the procedure itself in principle 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). The EDPS also takes note of the fact that the data subject can exercise the rights of access and rectification, as this enables individuals to control whether the data held about them is accurate (see Section 3.7).
However, as regards EP staff health data, the EDPS recommends establishing rules according to which EP staff health data is kept up to date and its accuracy ensured by inviting EP staff to fill in a new collection form at an interval corresponding to the four-year renewal of such data for MEPs (see also Section 3.5).

***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 (see Section 3.2) and fairness will be dealt with in relation to information provided to data subjects (see Section 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*".

- Data which is by its nature relevant for every mission will be erased at the end of the legislature for MEPs and on completion of service for EP staff. As regards MEPs, this seems to be a reasonable retention period for the purpose for which the data were collected[11]; as regards EP staff, the EDPS recommends establishing rules to ensure that EP staff health data is updated -and respective earlier health data be erased- at a similar five-year interval to ensure its accuracy (see also Section 3.4).
- Travel data relevant only to the specific mission will be deleted from the database upon return from that particular mission and all paper copies are destroyed after return from the mission. The exact length of the retention period will thus vary depending on the duration of the mission. The EDPS considers that this policy is in principle compliant with Article 4(1)(e) of the Regulation, but recommends that the EP establish specific rules for the deletion of travel data relevant only to the specific mission from the database upon return from that particular mission.

### 3.6. Transfer of data

- The EDPS notes that the transfer of data to recipients within the EP for the purposes specified for the SMD (see Section 2) complies with Article 7(1) of the Regulation. The EDPS recommends, however, that in accordance with Article 7(3) of the Regulation, each of the recipients is explicitly reminded that they should process the personal data they receive only for the purpose for which they were transmitted.
- Furthermore, a 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. In this case, Article 8 should be taken into account. **Article 8** of the Regulation 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,*

[11] For a comparable retention period regarding health data, see EDPS Opinion in case 2011-0933 of 16 March 2012.

*(...)(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 a medical emergency. Furthermore, since the data subject has given his/her consent to the processing, there would be no reason to assume, in principle, that his/her legitimate interests might be prejudiced.

- The processing may also involve a transfer to a third country. 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"*. However, Article 9(6) of the Regulation stipulates that: *"[b]y way of derogation from paragraphs 1 and 2, the Community institution or body may transfer personal data if: (...)(e) the transfer is necessary in order to protect the vital interests of the data subject; (...)"*. In the context of the processing operation at hand, it is obvious that such transfer happens to protect the vital interests of the data subject and is consequently to be regarded as covered by this derogation.

### 3.7. Rights of access and rectification

Article 13 of the Regulation provides a right of access to personal data being processed and Article 14 of the Regulation provides a right to rectification without delay of inaccurate or incomplete data. The rights of data subjects, including those of access and rectification are adequately provided for in Articles 8-11 of the implementing rules relating to the Regulation contained in the Bureau decision of 22 June 2005[12].

### 3.8. Information to the person concerned

With regard to data stemming from **"CODICT" and the travel agency**, the EDPS recommends informing data subjects at the time of collection of data for "CODICT" and the mission order that this data might also be used in the context of the SMD and to ensure that, on the basis of this information, data subjects can freely give their unambiguous consent.
The EDPS notes that data subjects are otherwise informed of most of the elements provided for in Articles 11 and 12 of the Regulation by means of the **collection form** (see above Section 2). However, the EDPS recommends that applicants should additionally be informed about the legal basis of the processing, the time limits for storing the data and the fact that data will be collected from "CODICT" and the travel agency.

### 3.9. Security measures

[...]

## 4. Conclusion

There is no reason to believe that there is a breach of the provisions of Regulation (EC) No 45/2001, provided the following considerations are fully taken into account. The EP must:

- ensure that data subjects at the time of collection of data for "CODICT" and the mission order are informed about and, on that basis, freely give their unambiguous consent to the use of that data in the context of the SMD;
- establish rules according to which EP staff health data is kept up to date and its accuracy ensured by (1) deleting respective heath data and (2) inviting EP staff to fill in a new collection form at an interval corresponding to the five-year renewal of such data for MEPs;

[12] See http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2005:308:0001:0006:EN:PDF

- establish specific rules for the deletion from the database of travel data relevant only to the specific mission upon return from that particular mission;
- remind each of the data recipients that they should process the personal data they receive only for the purpose for which they were transmitted in accordance with Article 7(3) of the Regulation;
- inform data subjects about the legal basis of the processing, the time limits for storing the data when collecting data through the collection form and the fact that data will be collected from "CODICT" and the travel agency.

Done at Brussels, 24 May 2012

(**signed**)

Giovanni BUTTARELLI
Assistant European Data Protection Supervisor