



Opinion on a notification for Prior Checking received from the Data Protection Officers of the CoR and the EESC regarding the processing operations to manage calls for tenders and contracts

Brussels, 15 September 2008 (Case 2008-346)

1. Proceedings

On 30 May 2008, the European Data Protection Supervisor (hereinafter "EDPS") received from the Data Protection Officers of the Committee of the Regions ("CoR") and of the European Economic and Social Committee ("EESC") a notification for prior checking regarding the data processing operations that take place in the context of the managing of calls for tenders and contracts ("the Notification").

On 25 July 2008, the EDPS sent the draft prior check Opinion to the data controllers of the CoR and the EESC for comments informing them that the month of August would not count for the two months period during which the EDPS has to issue a formal opinion. The data controllers responded on 10 September 2008.

2. Examination of the matter

2.1. The Facts

The *purpose* of the data processing operations is to manage calls for tenders and contracts between the EESC and the CoR on one side and third parties on the other side. In particular, the processing occurs regarding contracts and tenders which are managed by the unit Programming /Financial and Contractual Management of the Logistics and Translation Directorates of EESC and CoR.

The *primary responsibility* for the data processing lies within the unit Programming /Financial and Contractual Management of the Logistics and Translation Directorates of EESC and CoR (hereinafter "DLT Joint services COR-EESC").

The data processing operations are mainly manual and can be summarised as follows:

(i) Individuals who reply to invitations to tender provide personal information in the context of such replies. The information is provided in paper form. The replies are sent to the DLT Joint services COR-EESC.

(ii) Upon receiving such information the DLT Joint services COR-EESC assesses such information in the context of evaluating the tenders. An electronic list of tenderers is produced and deleted after the procedure is concluded.

(iii) After the contract is awarded, the data will be processed for the purposes of performance, management and follow-up of the contract.

The **types of data subjects** whose data are collected include all persons whose personal data are included in the submitted tenders and in contracts.

The **categories of data** collected and further processed include the following: (i) Identification data, which may include surname, first name, date (and place) of birth, sex, nationality, telephone number, email address; (ii) Data normally included in CVs, which includes education and professional experience. (iii) If the public contract exceeds a certain threshold, a recent extract from the judicial record is required.

Regarding **conservation** of data, according to the Notification, the personal information that relates to tenders which have been accepted is kept, together with the signed contract, both in paper form and in electronic form (scanned). This information is kept for five years. The personal information related to tenders which have not been accepted is deleted after the procedure is finished.

The data controller may **transfer personal data** gathered in the context of this processing operation to the following types of recipients: (i) To community institutions or bodies such as financial managing officers, verifying agents and authorising officers of DLT Joint services COR-EESC. In addition, information may be transferred to the European Court of Auditors, to the Financial Irregularities Panel and to OLAF. (ii) To other recipients such as members and observers of opening and evaluation committees.

As far as the **right to information** is concerned, the Notification explains that information is given in the invitation to tender letter and in the contract. Copies of both have been annexed to the Notification.

The information provided includes information about the purposes of the processing, the existence of the right of access and rectification, the recipients of the information and the right to have a recourse to the EDPS.

The rights of **access rights and rectification** are recognised and individuals are informed that these rights can be exercised by contacting the data controller.

As far as **security measures** are concerned, the data controller acknowledges that it has put technical measures in place to ensure the level of security appropriate to the risks, and to prevent any unauthorised disclosure or access, accidental or unlawful destruction or accidental loss or alteration, and to prevent all other unlawful forms of processing.

2.2. Legal Aspects

2.2.1. Prior Checking

Applicability of the Regulation. Regulation (EC) No 45/2001 applies to the "*processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system*" and to the processing "*by all Community institutions and bodies insofar as such processing is carried out in the exercise of activities all or part of which fall within the scope of Community law*"¹. For the reasons described below, all elements that trigger the application of the Regulation are present here:

First, the selection of the tenderers entails the collection and further processing of *personal data* as defined under Article 2(a) of Regulation (EC) No 45/2001. Indeed, as described in the Notification, personal data of individuals who are named in the answer for calls for tenders are

¹ See Article 3(2) of Regulation (EC) No 45/2001.

collected and further processed. Second, as described in the Notification, the personal data collected undergo *"automatic processing"* operations, as defined under Article 2(b) of Regulation (EC) No 45/2001 as well as manual data processing operations. Indeed, some of the personal information is collected in paper and processed to assess the most adequate tender. Finally, the processing is carried out by two Community institutions, in this case the CoR and the EESC, in the framework of Community law (Article 3(1) of Regulation (EC) No 45/2001). Therefore, all the elements that trigger the application of the Regulation are present.

Grounds for Prior Checking. Article 27(1) of Regulation (EC) No 45/2001 subjects to prior checking by the EDPS *"processing operations likely to present specific risks to the rights and freedoms of data subject by virtue of their nature, their scope or their purposes"*. Article 27(2) of the Regulation contains a list of processing operations that are likely to present such risks. This list includes, under paragraph (b), the processing operations intended to evaluate personal aspects related to the data subject, including his or her ability, efficiency and conduct. The processing operations that occur in the context of selecting tenders aim at evaluating tenders, including the professional capacity of the individuals mentioned in each tender, to carry out the tasks that are the object of the tender. In order to carry out such evaluation, the data controller will perform various assessment activities such as weighing up whether the individuals that are associated with a given tender are suitable to perform the tasks that will be required under the contract. In addition, prior checking is also necessary per application of Article 27 (1)(a) which subjects to prior checking the processing that concerns data relating to health and to suspected offences, offences, criminal convictions or security measures. In this case the processing may imply keeping information included in criminal records received from the tenderers. In sum, taking the above into account, clearly the data processing operations fall within Article 27(2) (a) and (b) and must therefore be prior checked by the EDPS.

Ex-post Prior Checking. Since prior checking is designed to address situations that are likely to present certain risks, the Opinion of the EDPS should be given prior to the start of the processing operation. In this case, however, the processing operations have already been established. This is not an insurmountable problem provided that all recommendations made by the EDPS are fully taken into account and the processing operations are adjusted accordingly.

Notification and Due Date for the EDPS Opinion. The Notification was received on 30 May 2008. The period within which the EDPS must deliver an opinion was suspended for a total of 16 days to allow for comments on the draft EDPS Opinion. In addition, the two months period deadline was also suspended during the month of August. The Opinion must therefore be adopted no later than 16 September 2008.

2.2.2. Lawfulness of Processing

Personal data may only be processed if legal grounds can be found in Article 5 of Regulation (EC) No 45/2001. As pointed out in the Notification, the grounds that justify the processing operation are based on Article 5(a), pursuant to which data may be processed if the processing 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"*.

In order to determine whether the processing operations comply with Article 5(a) of Regulation (EC) No 45/2001, two elements must be taken into account: first, whether either the Treaty or other legal instruments foresee a public interest task, and second, whether the processing operations carried out by the data controllers are indeed necessary for the performance of that task.

Legal Basis. In ascertaining the legal grounds in the Treaty or in other legal instruments that legitimise the processing operations notified for prior checking, the EDPS takes note of the following legal instruments:

(i) Council Regulation (EC, Euratom) No 1605/2002 of 25 June 2002 on the Financial Regulation applicable to the general budget of the European Communities, amended by Council Regulation (EC, Euratom) No 1995/2006 of 13 December 2006 and Council Regulation (EC) No 1525/2007 of 17 December 2007 L 343 9 27.12.2007 ("Financial Regulation").

(ii) Regulation (EC, Euratom) No 2342/2002 of 23 December 2002 laying down detailed rules for the implementation of Council Regulation (EC, Euratom) No 1605/2002 on the Financial Regulation applicable to the general budget of the European Communities, Amended by Commission Regulation (EC, Euratom) No 1261/2005 of 20 July 2005 and Commission Regulation (EC, Euratom) No 1248/2006 of 7 August 2006; and Commission Regulation (EC, Euratom) No 478/2007 of 23 April 2007 (hereinafter "Implementing Rules").

Upon analysis of the above legal framework, the EDPS is convinced that it provides an adequate legal basis for the processing at stake. These legal instruments foresee the data processing carried out by the CoR and the EESC for the purposes of selecting tenders and managing contracts in general. More particularly, these legal instruments foresee that the contracting authorities, in this case CoR and EESC may require information to proof the capacity of candidates within the scope of a tender² which will include the information normally provided in a CV. In particular, Article 137 of the Implementing Rules establishes that "*Evidence of the technical and professional capacity of economic operators may, depending on the nature, quantity or scale and purpose of the supplies, services or works to be provided, be furnished on the basis of one or more of the following documents: (a) the educational and professional qualifications of the service provider or contractor and/or those of the firm's managerial staff and, in particular, those of the person or persons responsible for providing the services or carrying out the works*". Furthermore, Article 134 of the Implementing Rules also foresee, for certain contracts, the collection of evidence, confirming that the individuals who will become contractual parties in a procurement procedure are not engaged in situations referred to in Article 93 or 94 of the Financial Regulation³ for which a criminal record is an appropriate instrument.

Necessity Test. According to Article 5(a) of Regulation (EC) No 45/2001, the data processing must be "*necessary for performance of a task*" as referred to above. It is therefore relevant to assess whether the data processing is "*necessary*" for the performance of a task, in this case, for the selection of the best tenders and managing contracts.

As outlined above, the Financial Regulation and Implementing Rules foresee the possibility for the CoR and the EESC to launch tendering procedures for the purposes of purchasing goods and services. To put this into practice, it is necessary and also foreseen for the CoR and the EESC to collect and further process personal information of tenderers. Unless the CoR and the EESC collect CVs and other relevant information, it would not be possible for them to verify the qualities of each of the tenders, including the professional capacity of the individuals who will perform tasks within a given tender in order to select the most suitable one.

² This legal framework also authorises the data controller to require information to prove other aspects such as financial, economic, and technical.

³ It includes situations such as if individuals are convicted of an offence concerning their professional conduct by a judgment which has the force of *res judicata*; if they have been guilty of grave professional misconduct proven by any means which the contracting authority can justify; they have been the subject of a judgment which has the force of *res judicata* for fraud, corruption, involvement in a criminal organisation or any other illegal activity detrimental to the Communities' financial interests.

In conclusion, it is the EDPS's view that the data processing that takes place in the context of selecting tenders and managing contracts is necessary towards ensuring the selection of the best tenders in a fair and transparent way.

2.2.3. Processing of Special Categories of Data

Article 10.1 of Regulation 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 Notification states that no data falling under the categories of data referred to in Article 10.1 are processed in the context of the data processing operations notified for prior checking.

Article 10.5 of Regulation (EC) No 45/2001 establishes that "*[processing of data relating to offences, criminal convictions or security measures may be carried out only if authorised by the Treaties establishing the European Communities or other legal instruments adopted on the basis thereof or, if necessary, by the European Data Protection Supervisor.*" According to the Notification, if the public contract exceeds a certain threshold, a recent extract from the judicial record is required. The EDPS considers that this processing is authorised by Article 93(1)(b) of the Financial Regulation and thus the requirement of Article 10(5) is met.

2.2.4. Data Quality

Adequacy, Relevance and Proportionality. Pursuant to Article 4(1)(c) of Regulation (EC) No 45/2001, personal data must be adequate, relevant and non excessive in relation to the purposes for which collected and/or further processed. This is referred to as the data quality principle.

The type of information requested to answer calls for tenders which includes details of qualification and experience seem appropriate for the purposes sought by the data processing. Only if the CoR and the EESC have information on the education and professional experience of the individuals who are associated with a tender, will the CoR and the EESC be able to select the best suited tender. In sum, the EDPS considers that the information collected complies with Article 4(1)(c) of Regulation (EC) No 45/2001.

Fairness and Lawfulness. Article 4(1)(a) of the Regulation requires that data must be processed fairly and lawfully. The issue of lawfulness was analysed above (see Section 2.2.2). The issue of fairness is closely related to what information is provided to data subjects which is further addressed in Section 2.2.8.

Accuracy. According to Article 4(1)(c) of the Regulation, personal data must be "*accurate and, where necessary, kept up to date, and every reasonable step must be taken to ensure that the data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified*". The implementing rules of the Financial Regulation, which indeed are of full application during the public procurement procedure, guarantee that data subjects have the right to access and to rectify data relating to them, so that the file can be as complete as possible. These rights are the means of ensuring that data are accurate and kept up to date. Thus the procedure guarantees the quality of the data. In this respect, see also Section 2.2.7.

2.2.5. Conservation of Data

Pursuant to Article 4(1)(e) of Regulation (EC) No 45/2001 personal data may be kept in a form which permits identification of data subjects for no longer than necessary for the purposes for which the data are collected and/or further processed.

Regarding *conservation* of data, according to the Notification, personal information related to the tenders that have been successful and have resulted in a contract, is kept for five years for the purpose of discharging the budget of the Committees for the year in which any resulting contract is concluded. The EDPS considers the conservation period of five years to be reasonable as this is the approximate period during which supporting documents are required to be kept by the Financial Regulation. Indeed, Article 49 of the Financial Regulation, as amended in 2007, establishes that "*The management systems and procedures concerning the keeping of original supporting documents shall provide for: (d) such documents to be kept for at least five years from the date on which the European Parliament grants discharge for the budgetary year to which the documents relate. Documents relating to operations not definitively closed shall be kept for longer than provided for in point (d) of the first subparagraph, that is to say, until the end of the year following that in which the operations are closed*". However, the EDPS would like to draw data controllers' attention to the last paragraph of Article 49 of the Financial Regulation according to which "*Personal data contained in supporting documents shall be deleted where possible when those data are not necessary for budgetary discharge, control and audit purposes*" and ask the data controller to assess whether this case allows for the deletion of the personal data (mainly CVs) contained in the winning tender.

The personal information related to tenders which have not been accepted is deleted after the procedure is finished, which is in line with Article 4(1)(e)

According to the Notification, the possibility for storing data for historical, statistical or scientific reasons appears to be excluded.

2.2.6. Transfers of Data

Articles 7, 8 and 9 of Regulation (EC) No 45/2001 set forth certain obligations that apply when data controllers transfer personal data to third parties. The rules differ depending on whether the transfer is made to (i) Community institutions or bodies (based on Article 7), (ii) to recipients subject to Directive 95/46/EC (based on Article 8), or (iii) to other types of recipients (based on Article 9).

According to the Notification, the data are transferred to community institutions or bodies such as financial managing officers, verifying agents and authorising officers of DLT Joint services COR-EESC. In addition, information may be transferred to the European Court of Auditors, to the Financial Irregularities Panel and to OLAF. The purposes of the transfer are to execute the payments of amounts due and to safeguard the financial interest of the Communities.

Article 7 of Regulation (EC) No 45/2001 applies insofar as the above recipients are Community institutions/bodies. This Article requires personal data to be transferred "*for the legitimate performance of tasks covered by the competence of the recipient*". In order to comply with this provision, in sending personal data, the controllers must ensure that (i) the recipient has the appropriate competences and (ii) the transfer is necessary. The EDPS considers that the transfers of information to the above for the purposes stated comply with the first and second requirements. Indeed, all the recipients have the competences to perform the tasks for which the data are transferred, which varies from authorising payments, fighting fraud, etc and the transfer of the data seems necessary for the recipients to carry out their respective tasks. Therefore the conditions of Article 7(1) are fulfilled.

As described in the facts, information about tenders, including the personal information, is transferred and further processed by members and observers of opening and evaluation committees which may be composed of external experts which will be located within the EU. Accordingly, Article 8 applies pursuant to which data may be transferred "*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*". The EDPS considers that such transfer is necessary for carrying out public procurement procedures. Consequently, the EDPS concludes that Article 8 of the Regulation is respected. Nevertheless, the EDPS recommends that the data controllers remind the recipients that the data must be kept confidential and must be used only for the purposes for which they were transferred.

2.2.7. Right of Access and Rectification

According to Article 13 of Regulation (EC) No 45/2001, the data subject shall have the right to obtain without constraint from the controller, communication in an intelligible form of the data undergoing processing and any available information as to their source. Article 14 of the Regulation provides the data subject with the right to rectify inaccurate or incomplete data.

According to the privacy statement, individuals are recognised such rights and are informed that they can be exercised by contacting the data controller. The EDPS notes that the Implementing rules are of full application during the whole public procurement procedures which ensure that the right of access and the right of rectification can be exercised by the data subjects. The EDPS consequently considers that Articles 13 and 14 of the Regulation are complied with.

2.2.8. Information to the Data Subject

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. 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.

In order to comply with this obligation, information to candidates is given with the invitation to tender letter and in the contract. The EDPS considers the provision of information through these channels as appropriate. The EDPS also finds it appropriate to provide the information before collecting any information from individuals.

The EDPS also reviewed the content of the information provided in the contract and invitation to tender and he considers that they satisfy the requirements of Articles 11 and 12 of Regulation (EC) No 45/2001.

2.2.9. Security measures

According to Articles 22 and 23 of Regulation (EC) No 45/2001, the controller and the processor must implement the appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented 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 prevent all other forms of unlawful processing. The CoR and the EESC acknowledge that they have adopted the security measures required under Article 22 of the Regulation.

3. Conclusion

There is no reason to believe that there is a breach of the provisions of Regulation 45/2001, provided the considerations in this Opinion are fully taken into account. In particular, COR and EESC must:

- Consider whether it may be possible to delete the personal data (mainly CVs) contained in the winning tender earlier than the five years conservation period.
- Remind the observers and experts that evaluate tenders that the information received must be kept confidential and must be used only for the purposes for which it was transferred.

Done at Brussels, 15 September 2008

(signed)

Peter HUSTINX
European Data Protection Supervisor