Guidelines on the processing of personal data in the context of public procurement, grants as well as selection and use of external experts

Introduction

These Guidelines are issued by the European Data Protection Supervisor (EDPS) in the exercise of the powers conferred on him in Articles 41(2) and 46(d) of Regulation (EC) No 45/2001 on the protection of personal data by the EU institutions and bodies[1] ("the Regulation"). They are based on the existing Opinions on the respective data processing operations by several EU institutions and bodies[2] and address the following procedures:

- **public procurement;**
- **grant awards and management;**
- **selection and appointment of external experts** on a basis of calls for expression of interest for tasks involving assistance in evaluation of grant applications, projects and tenders, and for providing opinions and advice in specific cases; as well as **conclusion and management of contracts** with the selected experts[3].

All these procedures are based on the EU Financial Regulation[4] and are launched by a publication of the respective call (for tender, for grant proposals or for expressions of interest). They all involve evaluation of the submitted applications according the same set of criteria provided therein in order to ensure the optimal use of EU financial resources. To the extent that the EU institutions and bodies process personal data relating to an identified or identifiable natural person within public procurement, grant procedures as well as selection and use of external experts, they are subject to the respect of the Regulation as an instrument of primary legislation[5]. This is notably the case when the tenderers or applicants are either natural persons or legal representatives of a company (legal person).

---

[1] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the EU institutions and bodies and on the free movement of such data.

[2] As provided in the Annex I and also available at the EDPS website (www.edps.europa.eu).

[3] Addressed in detail in point 9.

[4] Regulation (EU, Euratom) No 966/2012 of the European Parliament and of the Council of 25 October 2012 on the financial rules applicable to the general budget of the Union and repealing Council Regulation (EC, Euratom) No 1605/2002.

[5] According to Article 3(1) of the Regulation, it is applicable to the processing of personal data by EU institutions and bodies in the exercise of activities falling within the scope of the EU law. Any information relating to an identified or identifiable natural person should be considered as personal data in terms of Article 2(a) of the Regulation.

The main objective of the Guidelines is to offer guidance to all EU institutions and bodies in the processing of personal data by their administrative services in connection with the procurement, grants as well as selection and use of external experts. In this regard, the Guidelines also serve to assist the Data Protection Officers (DPOs) and controllers in their task of notifying the related data processing operations to the EDPS for prior checking where relevant.

The structure of the Guidelines follows closely the one which is used in the notification form for prior checking. In each section below, the common issues to all procedures are outlined first before possible procedure specific aspects are addressed.

1. Prior checking

All these procedures are intended to evaluate personal aspects of the applicants and tenderers (and/or their legal representatives) in terms of Article 27(2)(b) of the Regulation.

Indeed, their conduct is assessed according to the **exclusion criteria** laid down in Articles 106, 107 and 131 of the Financial Regulation, whereas their efficiency, professional and technical capacity (know-how, experience and reliability) is evaluated according to the **selection criteria** set out in Articles 147 and 148 of the Rules of Application[6].

Personal information about the absence of a conflict of interest for reasons involving family, emotional life, political or national affinity, economic or any other shared interest with the beneficiary[7], as well as information about (the absence of) certain convictions, such as for bankruptcy, professional misconduct, fraud or corruption, is also processed as foreseen in Article 27(2)(a) of the Regulation.

Furthermore, in certain cases data relating to health may be processed in connection with grant applications for additional funding due to special needs, such as in case of an Erasmus grant for a disabled student.

2. Lawfulness of the processing

The processing of personal data within procurement, grant and related expert selection procedures can be considered as necessary for the performance of a public interest task, namely the management and functioning of the respective EU institution or body and thus can be based on Article 5(a) of the Regulation[8].

[6] Commission Delegated Regulation (EU) No 1268/2012 of 29 October 2012 on the rules of application of Regulation (EU, Euratom) No 966/2012 of the European Parliament and of the Council of 25 October 2012 on the financial rules applicable to the general budget of the Union.

[7] As listed in Article 57(2) of the Financial Regulation, see Article 107(a) of the Financial Regulation. This issue will be further addressed in the forthcoming EDPS Guidelines on Conflict of Interest.

[8] To be read together with its recital 27 which states that processing of personal data for the performance of tasks carried out in the public interest by the EU institutions and bodies includes the

The legal bases confirming the lawfulness of the respective data processing operations can be found in the following legal acts:

- Regulation (EU, Euratom) No 966/2012 of the European Parliament and of the Council of 25 October 2012 on the financial rules applicable to the general budget of the Union and repealing Council Regulation (EC, Euratom) No 1605/2002 ("**Financial Regulation**") and in particular Articles 110, 131 - 133 and 204;
- Commission Delegated Regulation (EU) No 1268/2012 of 29 October 2012 on the rules of application of Regulation (EU, Euratom) No 966/2012 of the European Parliament and of the Council of 25 October 2012 on the financial rules applicable to the general budget of the Union ("**Rules of Application**") and in particular Articles 146 - 148, 201 - 202 and 287.

The EDPS notes that the processing of personal data in the procedures mentioned are considered as necessary for the performance of the EU institutions and bodies' obligations with respect to the above mentioned legal instruments. Therefore the processing of personal data may be considered as lawful on the basis of Article 5(a) of the Regulation.

3. Processing of Special Categories of Personal Data

As already indicated above, data relating to certain offences are processed in all procedures in question, whereas data relating to health may be processed in certain cases in the context of the grant procedures.

The processing of **data relating to offences and criminal convictions** in the form of an extract from the judicial record or declaration of honour can be considered as justified in terms of Article 10(5) of the Regulation since it is explicitly foreseen in Articles 106, 107 and 131 of the Financial Regulation, as well as Articles 141 – 145 and 287 of the Rules of Application. In principle, the applicants or tenderers have to demonstrate that they fully comply with the exclusion criteria set therein (such as bankruptcy, professional misconduct, fraud or corruption).

The processing of **health related data** submitted in connection with grant applications for additional funding due to special needs may be justified in terms of Article 10(2)(a) of the Regulation on condition that these data are submitted on a voluntary basis and thus with the data subject's consent.

In any case, only necessary information should be collected in order to certify the existence of special needs and the related costs. To this aim, the EDPS recommends that only one specific medical certificate from a national health service and an estimation of the additional costs made by a national medical centre is requested in this respect.

---

processing of personal data necessary for the management and functioning of these institutions and bodies.

Furthermore, the EDPS recommends that all staff members in charge of the processing of health related data are subjected to the specific obligation of secrecy equivalent to that of a health professional in terms of Article 10(3) of the Regulation. It is recommended that a specific professional secrecy declaration is established in this respect.

4. Data Quality

Pursuant to Article 4(1)(a), (c) and (d) of the Regulation, personal data must be processed fairly and lawfully, be accurate, as well as adequate, relevant and not excessive in relation to the purpose for which they are collected and further processed.

The accuracy of the administrative data processed in this context is notably ensured by the fact that they are provided by the data subjects themselves. Also, the rights of access and rectification help to ensure that the data processed are accurate and up to date (see point 7 below).

With respect to the existing selection and award criteria for the respective procedures, the processing of the following data may in principle be considered as necessary: name, date of birth, gender, nationality, VAT number, ID number, passport number, contract details, work experience / employment history, education, training and academic background and personal skills and competences (languages, technical skills). Staff collecting such data is nevertheless to be reminded that only relevant and necessary data may be collected and further processed.

As concerns the expert selection procedures, the collection of financial data in a financial identification form (such as bank account reference) together with the application documents may be considered as excessive in relation to the purpose of the procedure, i.e. the establishment of the list of external expert. Such data should only be collected at a later stage (only if and when the experts are selected).

5. Data Retention

According to Article 4(1)(b) and (e) of the Regulation, personal data may be kept in a form enabling 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. Further storage for historical, statistical or scientific purposes is possible only in an anonymous form (or with encrypted identity of the data subjects) on condition that the controller provides for appropriate safeguards that the personal data are not processed for any other purposes or used in support of measures or decisions regarding any individual.

The conservation of files of successful tenderers, grant applicants and experts for up to seven years after the signature of the respective contract, grant agreement or the end of the particular program can be considered as necessary for control and audit purposes in terms of Article 48(1)(d) and (2) of the Rules of Application, with the

exception of the extracts from the judicial records that can be kept only for two years after the accomplishment of the particular procedure[9].

The files of unsuccessful tenderers, grant applicants and experts may be retained only for up to five years after the end of the particular procedure to allow for all possible appeals.

In any case, according to Article 48(3) of the Rules of Application, personal data contained in supporting documents should be deleted where possible where these data are not necessary for budgetary discharge, control and audit purposes.

6. Transfer of Data

The data processed within procurement, grant and related expert selection procedures are transferred to several recipients in the same institution or body, to other institutions as well as to recipients outside the EU institutions or bodies.

The data transfers to members of the respective committees, the Executive Director and/or the Management Board can be considered as necessary for the accomplishment of the particular procedure, whereas the transfers to the internal auditors, the Court of Justice of the EU, EDPS, European Ombudsman, OLAF and the Central Exclusion Database can be considered, where relevant, as necessary for the performance of the respective supervisory or judicial task, all in line with Article 7(1) of the Regulation.

In order to ensure full compliance with the Regulation, the EDPS recommends that all internal recipients are reminded that the data should only be processed for the purpose for which they were transmitted (Article 7(3) of the Regulation).

The data transfers to external experts taking part in procurement and grant procedures on behalf of the respective institution or body have to be assessed in light of Articles 8 and 9 of the Regulation.

The transfers to external recipients established in the EU[10] are in compliance with Article 8(a) of the Regulation if their involvement in the respective procedure can be deemed necessary for the performance of a task in the area of public procurement or grants.

The data transfers to experts who are not subject to national law adopted pursuant to Directive 94/46 EC should be examined in light of Article 9 of the Regulation.[11]

The EDPS recommends asking explicitly for the applicant's consent that his personal data may be transferred within the particular procurement or grant procedure.

[9] See to this respect the letter on conservation of extracts from the judicial records sent by the EDPS to the management of all institutions and bodies on 12 March 2013 (2011-0482).

[10] Who are subject to the national law implementing the Directive 95/46 on the protection of individuals with regard to the processing of personal data and on the free movements of such data.

[11] See in this respect the forthcoming EDPS Guidelines on transfers of personal data to third countries and international organisations.

7. Rights of Data Subjects

The applicants and tenderers have the right to access, update or correct their personal data in accordance with Articles 13 and 14 of the Regulation. Whereas the right of access applies to both factual and evaluation data categories, the right of rectification is limited to the objective factual data (as the subjective evaluation statements cannot be factually wrong). The applicants and tenderers nevertheless have the possibility to complement the existing evaluation data by means of the respective appeal and review procedures.

Pursuant to Article 20(1) of the Regulation, these rights can be restricted in case it is necessary to safeguard, *inter alia*, an important economic interest of the EU, including budgetary matters, or the protection of the rights and freedoms of others (points b) and c)). Any restriction has to be applied restrictively on a case by case basis. In such a case, the data subject needs to be informed of the principal reasons of the restriction and of his right to have recourse to the EDPS as foreseen in Article 20(3) of the Regulation.

In this respect, the limitation of access to the aggregated evaluation results can be considered as justified as the access to evaluation results of other applicants (comparative results) or to opinions of individual members of the evaluation committee would undermine their respective rights.

Similarly, the limitation of the right to rectify ones data after the opening of tenders foreseen in Article 112 of the Financial Regulation[12] aiming to ensure transparency and equality of treatment can also be considered as justified on a basis of Article 20(1) of the Regulation.

8. Information to the Data Subject

In order to ensure transparency and fairness of the processing, the following information listed in Article 11 and/or 12 of the Regulation should be provided to the applicants and tenderers:

- identity of the controller,
- purpose of the processing,
- data categories,
- whether replies to the questions are obligatory or voluntary, as well as possible consequences of failure to reply,
- possible data recipients,
- existence of all data subjects' rights including procedures in place concerning access to the evaluation results upon requests and any limitation thereof,
- right to have recourse to the EDPS,
- legal basis of the processing,
- origin of the data, and
- applicable data retention periods.

[12] Read together with Article 160 of the Rules of Application on the exceptional nature of contact between contracting authorities and tenderers.

Due to the fact that this information should be provided either at the collection of data or before their first disclosure to a third party, the following means can be used to provide such information:

- specific privacy statement made available on the Internet,
- data protection clause in the on-line application forms,
- data protection clauses in the contract.

9. Processor

External experts assisting the EU institutions and bodies in evaluation of grant applications, projects and tenders, and providing opinions and advice in specific cases are considered to be processors in terms of Article 2(e) of the Regulation since they are processing personal data on behalf of these institutions and bodies.

Pursuant to Article 23 of the Regulation, a contract or legal act binding the processor to the controller should therefore be established stipulating, in particular,

- that the processor can act only on instructions from the controller, and
- that he has to comply with obligations of confidentiality and security set out in Articles 21 and 22 of the Regulation, unless he is already subject to these obligations provided in the respective national law transposing Articles 16 and 17(3) of Directive 95/46/EC.

For example, the following model contractual clauses could be used in this respect[13]:

"The contractor may act only under the supervision of the data controller, in particular with regard to the purposes of processing, the categories of data which may be processed, the recipients of the data and the means by which the data subject may exercise his rights.

The contractor shall not use confidential information and documents for any purpose other than the fulfilling of his obligations under the contract without prior written agreement of the contracting authority; ensure the protection of such confidential information and documents with the same level of protection it uses to protect its own confidential information, but in no case any less reasonable care; not disclose directly or indirectly confidential information and documents to third parties without prior written agreement of the contracting authority.

The contractor undertakes to adopt appropriate technical and organisational security measures having regard to the risks inherent to the processing and to the nature of the personal data concerned (...)."

[13]Articles II.5 and II.6 of the General Conditions for Service Contracts - see: http://intracomm.ec.testa.eu/budg/imp/procurement/imp-080-030-010_contracts_en.html.

10. Security measures

According to Article 22 of the Regulation, the controller should implement 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 processed. Such measures should in particular prevent any unauthorised disclosure or access, accidental or unlawful destruction or accidental loss, or alteration, and any other unlawful forms of processing.

In particular, appropriate access rights and access control should be put in place in terms of organisational measures, such as limited access to designated staff on a need-to-know basis, as well as technical measures, such as physical locks and/or secure connections and firewalls.