

DPO-2382.4 - RTD : Back-office notification: processing of data submitted by proposal Applicants and reviewers Experts in the context of Framework Programmes and other Programmes and Initiatives, managed by the Research General Directorate (DG RTD).

General information

Creation : 26/10/2007

Last updated : 06/06/2011

Registration : 06/06/2011

Status : Archived

Deleted : No

DG.Unit : RTD

Controller : SMITS Robert-Jan

Delegate :

DPC : BOURGEOIS Thierry, PENEVA Pavlina

Keywords :

Corporate : No

Language : English

Model : No Model

EDPS opinion (prior check) : No

Target Population :

DPC Notes :

Processing

1 . Name of the processing

Back-office notification: processing of data submitted by proposal Applicants and reviewers Experts in the context of Framework Programmes and other Programmes and Initiatives, managed by the Research General Directorate (DG RTD).

2 . Description

Cf. attachment "7) Description of processing", "Architecture" and "Architecture description".

List of attachments

- [7\) Description of processing v5.16.doc](#)
- [Architecture V5.13.pdf](#)
- [Architecture description V5.4.doc](#)

3 . Processors

N.A N.A|N.A N.A|N.A N.A|N.A N.A

4 . Automated / Manual operations

All processing operations have an automated part. This point covers back-office automated processing operations and supporting IT systems, see attachment in question 7. The front-office automated operations and supporting IT systems are covered by the front-office notification DPO-978 (DG RTD). This includes "Call Publishing" (Call Passport+CaP), "Submission and Evaluation of Proposals" (SEP), "Proposal Evaluation and Ranking" (ESS, until 2011, then through SEP), "Experts Registration" management on Cordis (EMPP), basic "Information Dissemination" on CORDIS and other websites accessible to Public, "Organisation Registration" and "Organisation Management" (URF/PDM/OMM).

The Local IT systems and supported back-office processing operations includes to date:

For both Experts and Applicants:

- SECUNDA: "Security Management" for local users

For Applicants:

- CaP: "Call Publication"
 - CPM: "Contract & Project Management"
 - NEF: "Negotiation module and back-office"
 - CORDA: "DG Reporting" for socio-economic data
- For experts:
- EMPP: "Expert Management Module"

The scope of the back-office manual processing operations performed by EU personnel or contractors on their behalf includes:

- Preparation of calls publication;
- Selection of Experts for proposal evaluation, or project review and monitoring purposes. Note that Experts' data are provided and maintained by Experts themselves;
- Managing Expert Contracts and Payments for services during proposal evaluation, or project review and monitoring. Bank account is provided by experts and verified by RTD;
- Managing the list of Proposals for further processing, including negotiation, and selected proposal lists approval;
- Managing the list of selected Projects, for further processing, including contract preparation, and initial payments;
- Managing the projects and further processing, including deliverables, contract amendments, and intermediate or final payments;
- Managing reporting requirements for operation at Project, Operational Unit, Directorate or RTD level;
- Carrying out Projects auditing, to assess whether or not all relevant legal obligations were properly followed;
- Managing publication and dissemination of results;
- Managing RTD users access to supporting IT systems.

5 . Storage

The data is stored at the DG DIGIT data centre, physically under the control of DG DIGIT. The data can be transferred to local DG data centres operating under the same rules as the Digit data centre. It is stored in various computer readable formats, including on magnetic and optical storage media.

The proposal data may also be stored in paper format the Project Officer's (PO) office, the AFUs (Administration & Finance Units) office, as well as archived at the Commission Zaventem storage facility.

6 . Comments

DG RTD staff of operational Units may request and get access to information provided by Applicants and Experts. However, payments are approved and carried forward by the Administration and Finance Units (AFU) only.

Purpose & legal basis

7 . Purposes

The purpose of the processing is:

- To manage the Commission's administration of projects submitted for funding or funded through the Research Framework Programmes.
- To manage the Research Framework Programmes as a whole, in accordance with the applicable regulation (s).
- To manage other (non-FP) Programmes funded by Research Family's DGs as a whole, in accordance with the applicable Legal Framework.

8 . Legal basis and Lawfulness

Cf. attachment "11) Legal basis of processing".

The data processing is considered lawful, because it is necessary to:

- Meet requirements of the legal instruments mentioned above
- Ensure compliance of Commission with legal obligations
- Perform a contract with the data subject (or take steps prior to entering into contract) as described in points (a), (b) and (c) of Art 5 of Regulation (EC) 45/2001.

For access to the Commission's database of potential experts by:

- Public research funding bodies from the Member States and the States associated to the Research Framework Programmes or to other Programmes and Initiatives,
- Commission departments not involved in the administration of the research Framework Programmes or of other Programmes and Initiatives,

For paper and Internet publication of pictures, age, nationality and short curriculum vitae of funded projects coordinators/leaders or principal investigators (successful applicants),

the data subject has given his prior unambiguous consent. Either the data subject opted in at the time of the registration, or the data subject has signed a dedicated declaration agreement (cf. model attached to question 15) Information to data subjects). The data processing is subject to prior approval of the data subject through two opt-in options at the time of the registration, as described in points (d) of article 5 and 6.(a) of article 9 of Regulation (EC) 45/2001.

Articles 20 (Exemptions and restrictions) and 27 (Prior checking by the EDPS) are not applicable.

[List of attachments](#)

- [11\) Legal basis of processing v5.16.doc](#)

Data subjects and Data Fields

9 . Data subjects

See point 16).

10 . Data fields / Category

Cf. attachment "17) Data fields of data subjects".

See point 17) above.

[List of attachments](#)

- [17\) Data fields of data subjects v5.16.doc](#)
- [21\) Category\(ies\) of recipients v5.16.doc](#)

Rights of Data Subject

11 . Mandatory Information

Information to the Data Subjects as described in articles 11-12 under 'Information to be given to the Data subjects' is provided in service specific privacy statements (SSPSs) displayed on websites that collect personal data of:

- Applicants:

<http://ec.europa.eu/research/participants/portal/appmanager/participants/portal>

<https://www.epss-fp7.org/epss/welcome.jsp>

[https://webgate.ec.europa.eu/nef/frontoffice/project/project number/view](https://webgate.ec.europa.eu/nef/frontoffice/project/project%20number/view)

- Experts: within the scope of the front-end notification of REA.

Furthermore, applicants who have not opted-in at the time of their registration and who are granted may be offered to give their prior and unambiguous consent to the publication of their picture, nationality, age and short curriculum vitae at a later stage (cf. section 17), through signature of a declaration of agreement.

[List of attachments](#)

- [SSPS Applicants v6.9.doc](#)

12 . Procedure to grant rights

Data subjects may contact the data Controller to exercise their rights under articles 13-19, and are informed that any update of the process and related notification are published on the website of the commission's data protection officer (http://ec.europa.eu/dataprotectionofficer/register/index.cfm?TargetURL=D_REGISTER)

13 . Retention

For experts selected and for organisations retained for funding and grant agreements, personal data (on papers and registered in data bases) are kept as required by the Commission's Common Retention List (SEC (2007)970), i.e. 10 years after the end of the project. As experts may themselves update or delete their personal data online, personal data not updated after 10 years will be removed from the databases.

For organisations which are not granted, personal data are kept for 3 years and erased after this period.

14 . Time limit

Blocking or rectifying data may be made by the Experts themselves and on request for Applicants, as mentioned to the data subjects in the corresponding SSPS (see point 15). The password they chosen by Experts during registering will allow them to log in to the system and update their personal information or delete their registration.

15 . Historical purposes

Project files are kept in the archives in Zaventem according to Commission rules.

Recipients

16 . Recipients

Individuals falling in the categories listed in point 21).

Cf. attachment "21) Categories of recipients" attached to question 17).

17 . Transfer out of UE/EEA

Not applicable - no transfer of personal data to third party countries, unless publication on the CORDIS website of limited personal data as explained under question 21).

Security measures

18 . Technical and organizational measures

General comment applying to all sub-points: • Data processing by Experts, e.g., viewing or modifying, is limited via registration and access control to areas with own information only. • Data processing for proposal applicants is limited via registration and access control to own areas only and in submitting proposals. • Data processing is on the central IT infrastructure of the Commission (data centre and data network) maintained by DG DIGIT, following the rules, procedures, organisation, and security rules of DG DIGIT. • Physical access control to network, servers and media is managed by DG DIGIT. Access to the data is only available to processors and to registered users as approved by their hierarchy through a separate access control and security module (SECUNDA). The security module logs which user has requested access to the system, together with date and timestamp. Authentication is based on the DIGIT ECAS mechanism.

a) preventing any unauthorised person from gaining access to computer systems processing personal data; :yes - No specific measure - see general comments in point 31).

b) preventing any unauthorised reading, copying, alteration or removal of storage media; :yes - No specific measure - see general comments in point 31).

- c) preventing any unauthorised memory inputs as well as any unauthorised disclosure, alteration or erasure of stored personal data; :yes - No specific measure - see general comments in point 31).
- d) preventing unauthorised persons from using data-processing systems by means of data transmission facilities; :yes - No specific measure - see general comments in point 31).
- e) ensuring that authorised users of a data-processing system can access no personal data other than those to which their access right refers;:yes - No specific measure - see general comments in point 31).
- f) recording which personal data have been communicated, at what time and to whom;:yes - No specific measure - see general comments in point 31).
- g)ensuring that it will subsequently be possible to check which personal data have been processed, at what time and by whom; :yes - No specific measure - see general comments in point 31).
- h) ensuring that personal data being processed on behalf of third parties can be processed only in the manner prescribed by the contracting institution or body; :yes - No specific measure - see general comments in point 31).
- i) ensuring that, during communication of personal data and during transport of storage media, the data cannot be read, copied or erased without authorisation; :yes - No specific measure - see general comments in point 31).
- j) designing the organisational structure within an institution or body in such a way that it will meet the special requirements of data protection; :yes - No specific measure - see general comments in point 31).

General comments applying to all sub-points:

- Organisational structures have been set up in accordance with the principles of the Regulation 45/2001.
- Access to personal data collected is only granted to users "who need to know" through UserId/password.
- Where personal data are collected through an external company, the latter has to adopt organisational measures in order to guarantee the data protection and confidentiality required by the Regulation 45/2001.
- It could be that the data subject may opt-out for the publication of certain of his/her personal data, while the access to the rest of the personal data collected is only granted through UserId/password to a defined population of users or through the offered opt in options for another population of users (cf. point 7).

See general comment in question 31).

General comments applying to all sub-points: - Organisational structures have been set up in accordance with the principles of the Regulation 45/2001. - Access to personal data collected is only granted to users "who need to know" through UserId/password. - Where personal data are collected through an external company, the latter has to adopt organisational measures in order to guarantee the data protection and confidentiality required by the Regulation 45/2001. - It could be that the data subject may opt-out for the publication of certain of his/her personal data, while the access to the rest of the personal data collected is only granted through UserId/password to a defined population of users or through the offered opt in options for another population of users (cf. point 7).

- a) preventing any unauthorised person from gaining access to computer systems processing personal data; :General comments applying to all sub-points: - Organisational structures have been set up in accordance with the principles of the Regulation 45/2001. - Access to personal data collected is only granted to users "who need to know" through UserId/password. - Where personal data are collected through an external company, the latter has to adopt organisational measures in order to guarantee the data protection and confidentiality required by the Regulation 45/2001. - It could be that the data subject may opt-out for the publication of certain of his/her personal data, while the access to the rest of the personal data collected is only granted through UserId/password to a defined population of users or through the offered opt in options for another population of users (cf. point 7). No specific measures - see general comments in points 31) and 32).
- b) preventing any unauthorised reading, copying, alteration or removal of storage media; :No specific measures - see general comments in points 31) and 32).
- c) preventing any unauthorised memory inputs as well as any unauthorised disclosure, alteration or erasure of stored personal data; :No specific measures - see general comments in points 31 and 32.
- d) preventing unauthorised persons from using data-processing systems by means of data transmission facilities; :No specific measures - see general comments in points 31 and 32.
- e) ensuring that authorised users of a data-processing system can access no personal data other than those to which their access right refers;:No specific measures - see general comments in points 31 and 32.
- f) recording which personal data have been communicated, at what time and to whom;:No specific measures - see general comments in points 31 and 32.
- g)ensuring that it will subsequently be possible to check which personal data have been processed, at

what time and by whom; :No specific measures - see general comments in points 31 and 32.

h) ensuring that personal data being processed on behalf of third parties can be processed only in the manner prescribed by the contracting institution or body; :No specific measures - see general comments in points 31 and 32.

i) ensuring that, during communication of personal data and during transport of storage media, the data cannot be read, copied or erased without authorisation; :No specific measures - see general comments in points 31 and 32.

j) designing the organisational structure within an institution or body in such a way that it will meet the special requirements of data protection; :No specific measures - see general comments in points 31 and 32.

19 . Complementary information

Cf. enclosures: note from the Controller to the processors (all directorates) and its annexes, plus the Guide to Financial Issues relating to FP7 Indirect Actions.

List of attachments

- [Note 24839 du 23-10-2007.pdf](#)
- [Annexe 1 \(contexte et terminologie\).pdf](#)
- [Annexe 3.1.doc](#)
- [Annexe 5 \(check-list\).pdf](#)
- [FP7 Ind Actions.pdf](#)