

DPO-978.4 - RTD : Front-office notification: processing of data submitted by proposal Applicants in the context of Framework Programmes and other Programmes and Initiatives managed by the Research Family's DGs (RDGs) and related Executive Agencies (EAs) and Joint Undertakings (JUs)

General information

Creation : 06/02/2006

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

Front-office notification: processing of data submitted by proposal Applicants in the context of Framework Programmes and other Programmes and Initiatives managed by the Research Family's DGs (RDGs) and related Executive Agencies (EAs) and Joint Undertakings (JUs)

2 . Description

Cf. attachements "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

DEASY Declan|SAFFAR Danielle|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 cover front-office automated processing operations and supporting IT systems (see attachment in point 7.) for applicants and participants. The front-office operations relating to experts are covered by the Research Executive Agency (REA), owner of the corresponding IT application, EMPP: "Expert Management in the Participant Portal".

The back-office processing operations and supporting systems are covered in the (local) back-office notifications of each Research family's DG.

The IT systems and supported front-office operations include:

- Cordis portal & Call Passport: "Call Publishing"
- Cordis portal: "External User Helpdesk"
- SEP: "Submission and Evaluation of Proposals"
- ESS: "Proposal Evaluation & Ranking" (until 2011, then through SEP)

- Cordis portal: "Publication of NCP names"
- CCM2: "Management of Codes and Calls reference data"
- SECUNDA: "Security Management" for local users
- OMM: "Organisation Management Module"
- PINOCCHIO/RIVET: "Evaluation Support" (for Research DGs)
- CaP: "Call Publishing"
- PDM/URF: "Organisations Registration/Verification/Validation"
- EFP: "Evaluation Facility Planning"
- NEF: "Negotiation Form"
- IAM: "Identity and Access Management"
- SESAM: management of accesses to SED, ESS, ARI, MCA
- FORCE (Form C)

Some of these services are embedded into the so-called "Participant Portal" (cf. attachments to question 7) Description of processing).

The scope of the front-office manual processing operations performed by EU personnel or contractors on their behalf is rather limited to certain areas mentioned below. Manually initiated transfer of data between systems is not considered as a processing operation and it is not mentioned here. The following processing operations are considered:

- Updating the CCM2 codes and calls reference data after a new call or RDG reorganisation;
- Publishing a call after input is received via the Call Passport system and CaP;
- Organisation of data management, including research and identification of duplicate entries, verification and validation for organisation legal status following adequate background research, and management of unique organisation (participant) ids;
- Keeping paper documents storage, e.g. on organisation legal status.

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 form, and they are transferred to the appropriate DG for further processing.

Organisation validation data (legal of financial) may also be stored in paper form, but they remain under the control of the Research Executive Agency (REA).

6 . Comments

The responsibility for front-office operations and supporting IT systems is limited to the operations supported by RTD. Processing operations on data collected by front-office systems like Expert selection, and proposal evaluation and ranking is really performed by the Research DGs and related EAs and JUs, and are covered in their respective notifications for back-office processing operations (cf. question 8).

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 DGs and related EAs and JUs as a whole, in accordance with the applicable regulation(s).

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 and ensure compliance of Commission with legal obligations as described in point (b) of article 5 of Regulation (EC) 45/2001;
- Perform a contract with the data subject (or take steps prior to entering into contract) as described in points (c) of article 5 of Regulation (EC) 45/2001.

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.

[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) Categories of recipients".

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.

- 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>

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 (cf. section 17) at a later stage, 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 through the contact points indicated at the time they register or as indicated in the appointment letter/grant agreement 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 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. 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 falling could be done on request, as mentioned in the Specific Privacy Statements (see point 15).

Regarding erasing Proposal Contact, this can be done by the concerned persons themselves via the web interface and their password, as set during 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. "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.

Security measures

18 . Technical and organizational measures

Access to the data is only available to registered users as approved by their hierarchy through a separate access control module managed by RTD (ECAS and SECUNDA for the OMM). The security module logs which user has requested access to the system, together with date and timestamp. General comment applying to all sub-points: • 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 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; :No specific measure - see general comments in point 31).

- b) preventing any unauthorised reading, copying, alteration or removal of storage media;** :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;** :No specific measure - see general comments in point 31
- d) preventing unauthorised persons from using data-processing systems by means of data transmission facilities;** :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;**:No specific measure - see general comments in point 31).
- f) recording which personal data have been communicated, at what time and to whom;**: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;** :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;** :See general comments in point 31), also • IT administrators have access to personal data
- 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 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;** :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 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).

- 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 User Id/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 User Id/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

Enclosures: the Guide to Financial Issues relating to FP7 Indirect Actions and the note and its annexes sent by the Controller to his processors.

Note to points 23-26:

OPOCE is responsible for the relations with the data processor in respect of CORDIS, the EMPP module and some elements of the SESAM module; REA is responsible for the management of the SEP service and the Central Validation Team (CVT); DIGIT is the data processor in respect of the other modules.

List of attachments

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