

# DPO-978.2 - RTD : Front-office notification: processing of data submitted by Experts and proposal Applicants in the context of Framework Programmes and other Programmes and Initiatives managed by the Research Family's DGs (RDGs)

## General information

**Creation** : 06/02/2006

**Last updated** : 18/09/2008

**Registration** : 18/09/2008

**Status** : Archived

**Deleted** : No

**DG.Unit** : RTD.G.5

**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 Experts and proposal Applicants in the context of Framework Programmes and other Programmes and Initiatives managed by the Research Family's DGs (RDGs)

### 2 . Description

Collection and registration of the information needed to manage Framework Programs and other Programmes and Initiatives, in accordance with the appropriate regulations, from the publishing of calls, initial collection of personal data from proposal Applicants and Experts to evaluate these proposals, up to the point where collected data are sent to individual research DGs for further processing as projects until their closure. These further processing operations are covered under the so-called specific back-office notifications introduced by each Research DG. Please see attachments for the detailed description of the processing operations (see also attachment under point 7.).

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

List of attachments

- [Some explanation relating to front-back architecture V0.2.doc](#)
- [Architecture V2 PDF.pdf](#)
- [Detailed description of the processing operations \(point 7\).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.). The back-office processing operations and supporting systems are covered in the 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"
- EPSS: "Electronic Proposal Submission"
- ESS: "Proposal Evaluation & Ranking"
- Cordis portal: "Publication of NCP names"
- CCM2: "Management of Codes and Calls reference data"
- SECUNDA: "Security Management" for local users
- OMM: "Organisation Management Module"
- EMC: "Expert Registration"
- PINOCCHIO/RIVET: "Evaluation Support" (for Research DGs)
- PDM/URF: "Organisations Registration/Verification/Validation"
- EFP: Evaluation Facility Planning

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:

- Establishing and approving lists of Experts to be invited to evaluations
- Providing help to Experts e.g., in case of EMC access password reset or other access related problems
- 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
- 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 centers operating under the same rules as the Digit data center. 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 RTD/T5 unit.

Organisation validation data (legal of financial) may also be stored in paper form, but they remain under the control of the RTD/T5 unit archiving at the Commission Zaventem storage facility.

## 6 . Comments

The responsibility for front-office operations and supporting IT systems is limited to the operations supported by RTD/T5. Processing operations on data collected by front-office systems like Expert selection, and proposal evaluation and ranking is really performed by the Research DGs for now, 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 as a whole, in accordance with the applicable regulation(s).

## 8 . Legal basis and Lawfulness

Cf. attachement for the list.

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 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,

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](#)

- [Legal basis \(point 11\).doc](#)

## Data subjects and Data Fields

### 9 . Data subjects

See point 16.

### 10 . Data fields / Category

The IT applications manage general personal data required to achieve the purposes of the processing.

They do not manage any sensitive personal data in the meaning of Article 10 of Regulation (EC) N° 45/2001 of the 18 December 2000.

IT administrators have access to user identification such as login identifier and access rights, as well as information necessary for IT system security and user access auditing reasons.

For applicants, the data collected are:

- Last name, First name
- Title, Gender
- Department/Faculty/Institute/Laboratory name
- Phone, Mobile phone
- E-mail, Fax
- Address, if different from organisation address

And, if proposal is selected, then additional information is be collected:

- Bank account reference (IBAN and BIC codes),
- VAT no (where applicable)

Data relating to expert evaluators and reviewers:

- First Name, Name,
- Phone number, fax number, e-mail address,
- Expert type
- Passport n°, Place/Date of Birth,
- Previous Family Name, Employment details (including whether currently employed, current employer, and 5 previous employers),
- Candidature reference, previous proposal submitted & programme,
- Professional experience, Research interest, and expertise (in keywords),

and, in case of appointment:

- Bank account reference (IBAN and BIC codes),
- VAT no (where applicable)

Experts can select whether or not (opt-in option) they authorise other Commission departments not involved in

the administration  
of the research Framework Programmes or of other Programmes and Initiatives, and public research funding bodies from the  
Member States and the States associated to the Research Framework Programmes or to other  
Programmes and Initiatives to access the data submitted by them. This data is entered by experts themselves  
on  
the EMC or Participant Portal web site maintained by CORDIS under a service contract with the EC.

See point 17 above.

[List of attachments](#)

- [Categories of recipients \(point 21\).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 displayed on websites that collect personal data (for Applicants: <https://ec.europa.eu/research/participants/urf/secure/new/initialRegistrationRequest.do> and <https://www.epss-fp7.org/epss/welcome.jsp>, for experts: <https://cordis.europa.eu/emmp7/index.cfm?fuseaction=wel.welcome>).

[List of attachments](#)

- [V2.1 200800618 SSPS EXPERTS \(clean\).doc](#)
- [V3.1 20080618 SSPS APPLICANTS EPSS \(clean\).doc](#)
- [V3.1 20080618 SSPS APPLICANTS URF \(clean\).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](http://ec.europa.eu/dataprotectionofficer/register/index.cfm?TargetURL=D_REGISTER)).

### 13 . Retention

For Applicants:

For proposals retained for funding and grant agreement, data are kept for the longer one of the possible following periods:

- Duration of the individual projects (plus 10 years after the end of the project to allow for audits)
- Duration of the Research Framework Programmes and Initiatives (plus 5 years on individual projects to allow for audits)
- Duration of an audit (if one is in progress)

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

For Experts:

Personal data are kept 10 years after their last update, unless of course Experts delete them themselves.

### 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 and Experts personal data, 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.

Please see note from the Controller to the processing services in attachment to question 37.

Because of a lack of space, please see the requested information in attachment to point 17: "Categories of recipients (point 21)".

### 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 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 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;** :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

Note to points 23-26:

OPOCE is responsible for the relations with the data processor in respect of the EMC module and some elements of the SESAM module; 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](#)