

# DPO-978.1 - RTD : FP6/7 IT System (core functionality)

## General information

**Creation :** 06/02/2006

**Last updated :** 26/04/2006

**Registration :** 26/04/2006

**Status :** Archived

**Deleted :** No

**DG.Unit :** RTD.R.4

**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

FP6/7 IT System (core functionality)

### 2 . Description

Processing of the information needed to manage FP6 and FP7 proposals and projects in accordance with the appropriate regulations throughout their whole lifecycle, including:

- Submission and evaluation of proposals (\*)
- Ranking, negotiation and decision of the proposals (\*)
- Contract preparation, generation, validation, execution and monitoring
- Transferring financial transactions to and from the Commission's accounting system for further validation and processing
- Publication of project summaries on Cordis portal
- Statistics, reporting and information relating to management and monitoring of the Research Framework Programmes.

The processing will be extended to cover FP7 (subject to the adoption of the legal basis for FP7, which needs to be added to point 11 below), and other activities of the Research DGs relating to management of grants.

The data processed does not fall under Article 27, and does not require prior checking by the European Data Protection Supervisor.

This notification only covers activities under the responsibility of the ITMO.

(\*): These steps include automated processing that is covered by a service contract managed by the EC (see point 8)

None of the processing operations fall under the Article 27.

### 3 . Processors

DEASY Declan|SAFFAR Danielle

### 4 . Automated / Manual operations

The system contains a number of modules with different functions, including some service contracts managed by the EC, namely, the ESP (External Service Provider for Evaluations), and EPSS (Electronic Proposal Submission System).

This notification covers the functionality from the following modules:

- CCM: Codes and Calls Module
- CPM: Contract and Project Management
- DESIS: Data Exchange Sub-Information System
- EMI/EMC: Expert Management Module
- DWH: Data warehouse
- OMM: Organisation Management Module
- PMT/Prima: Proposal Management Tool
- SEC: Security Module
- CIRCA: Documents Exchange System
- SESAM : DAM (Data Aggregation Module), QUEST (questionnaire submission & consultation), and QUEST-I (internal questionnaire management)

This notification does not cover any automated "local" processing by the Commission services that may be undertaken in operational and administrative / financial units of the Research Directorates General

In the scope of the ITMO, the only manual processing operations are ancillary to the automated processing operations mentioned above, for example, to transfer data between the modules mentioned above and to verify correct operation of the automated processing.

Manual processing of personal data may be carried out by the appropriate operational and administrative / financial units. This processing falls outside the scope of this notification.

## 5 . Storage

The data is stored at the DG DIGIT data centre, physically under the control of DG DIGIT. It is stored in various computer readable formats, including on magnetic and optical storage media.

## 6 . Comments

Note: "ITMO" stands for "IT Management Office", and refers to unit DG RTD/R/5

# 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) projects funded by DG RTD (and other Research DG).
- To disseminate key results of the research funded by the EU.
- To provide information as input for future policy making.

## 8 . Legal basis and Lawfulness

- Council Regulation (EC) N° 1513/2002 of 27 June 2002 concerning the sixth Framework Programme of the European Community for research, technological development and demonstration activities, contributing to the creation of the European Research Area and to innovation (2002 to 2006)
- Council regulation (EC, Euratom) N° 2002/668 of 3 June 2002 concerning the sixth Framework Programme of the European Atomic Energy Community (Euratom) for nuclear research and training activities, also contributing to the creation of the European Area (2002 to 2006)
- Various implementation regulations, and general regulations such as the Financial Regulations

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.

## Data subjects and Data Fields

### 9 . Data subjects

See point 16

### 10 . Data fields / Category

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

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

The data managed for all data subjects are:

- Name, First name
  - For anyone who has access to the system: User identification (login identifier, account reference) and information necessary for system security or audit reasons
  - Gender, Nationality, Language
  - Title, Function, Role
  - Contact details (Address, work department, country of residence, email address, business and mobile telephone numbers, fax n°, etc)
  - If the person receives payment: Bank account reference (IBAN and BIC codes), VAT n° (where applicable)
- Data relating to expert evaluators and reviewers:

- 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)
- Languages written, spoken and read

Experts can select whether they authorise other Commission departments, Member States and States associated with the FP to access the data submitted by the expert. This data is entered by experts themselves on the EMC web site maintained by CORDIS under a service contract with the EC.

Data relating to Commission staff and intra-muros experts:

- EC Directorate General, Directorate, Unit, Office location

See point 17 above

## 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 Subject' is provided in the text of the general conditions of the contract text provided to the contracting parties, and in the text displayed on web sites that collect personal data.

### 12 . Procedure to grant rights

- Data subjects may contact the Data controller to exercise their rights under articles 13-19.
- The procedures followed will vary depending on the nature of the request.
- There is no charge for this request.

### 13 . Retention

Data are kept for the longer of:

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

### 14 . Time limit

Blocking or rectifying data falling under the conditions of Art 13 to 16 of EC Regulation 45/2001 could be done on request.

### 15 . Historical purposes

Not applicable

## Recipients

### 16 . Recipients

Individuals falling in the categories listed in point 21.

- Internal authorised Commission staff and others that are working on behalf of the Commission to manage research projects within the Research Framework Programmes. They will include staff from DG RTD, ENTR, FISH, INFSO or TREN, and certain horizontal DGs

- Institutions involved in monitoring the Commission's operations (for example, Court of Auditors)

- Other structures associated with the Research Framework Programmes, such as Programme Committees.

A very limited subset of data is held at CORDIS (contact details of the main coordinator), in order to allow contacts between interested parties and the research consortium. Lists of experts who participated in evaluations are published through CORDIS after the evaluation is complete, giving name, gender nationality and organisation. The webpage on which experts can register themselves for consideration for appointment as experts ([http://www.cordis.lu/experts/fp6\\_candidature.htm](http://www.cordis.lu/experts/fp6_candidature.htm)) contains a statement advising them that these details may be published.

Personal data is not transferred to third parties outside the EU.

### 17 . Transfer out of UE/EEA

There are no transfers to third party countries not subject to Directive 95/46/EC (Article 9). Transfers to other community institutions and bodies and to member states are covered under point 20.

## Security measures

### 18 . Technical and organizational measures

General comment applying to all sub-points: 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 registered users as approved by their hierarchy through a separate access control module managed by ITMO. The security module logs which user has requested access to the system, together with date and timestamp

**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
- 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 comment applying to all sub-points:

Organisational structures have been set up in accordance with the rules of the DPO. Access is only granted by the security administrator within the policy guidelines, and to users approved by management.

The organisational measures recognise that the physical infrastructure is under the control of DG DIGIT. The organisational measures therefore concentrate on access control through the Commission's desktop equipment.

See general comment in point 31

General comment applying to all sub-points: Organisational structures have been set up in accordance with the rules of the DPO. Access is only granted by the security administrator within the policy guidelines, and to users approved by management. The organisational measures recognise that the physical infrastructure is under the control of DG DIGIT. The organisational measures therefore concentrate on access control through the Commission's desktop equipment.

- 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.

