



EUROPEAN COMMISSION
JOINT RESEARCH CENTRE

Resources
Recruitment and Training Unit

February 2012

MANAGEMENT OF SELECTION AND RECRUITMENT FILES FOR GRANTHOLDERS AT THE JOINT RESEARCH CENTRE (JRC) Privacy Statement

1. Identity of the controller

Personal data supplied by candidates as part of a selection and recruitment procedure for grantees are collected and further processed according to Regulation (EC) 45/2001 of the European Parliament and of the Council of 18/12/2000 on the protection of individuals with regard to the processing of personal data by Community institutions and bodies on the free movement of such data. The Controller of the processing operation on personal data is the Joint Research Centre represented in this case by the Director of Resources. The Heads of the Resource Management Units (RMUs) of the Institutes and the Head of the Recruitment and Training Unit (RTU - Ispra) of the JRC are responsible for internally managing the processing operation on behalf of the controller.

This privacy statement refers to the management of the selection and recruitment of grantees at the Ispra, Geel, Karlsruhe, Petten and Seville sites.

2. Purposes of the processing operation for which the data are intended

The grantee process commences with the launch of a call published on the JRC Internet website(s) and covers the selection and recruitment processes (managed by the RMUs and RTU).

At the application phase (via ESRA¹):

Basic personal data are collected such as surname, name, maiden name (if applicable), address, telephone number, e-mail address, gender, nationality, country/place of birth and date of birth. Other data gathered relate to university education, languages, work experience, prior work experience with the Commission, an additional category (free field) and a motivation letter (compulsory).

At the selection phase (if invited for interview with reimbursement of expenses)

Invitation note requires the return of a financial identification and a legal entity form with a copy of the candidate's passport/identity card and a declaration from the candidate's bank confirming details of his/her bank account. In addition, the request for reimbursement form must be compiled.

At the recruitment phase:

The data below are used to prepare and finalise the selected grantee's file and to allow for his/her entry into service:

- Curriculum Vitae.
- Copy of passport/identity card.
- Copy of university degrees, proof of enrolment in a university doctoral studies programme (for category 20 only); evidence proving minimum research experience (for category 30 and 40 only) if applicable.
- Professional experience form duly filled in and proof of the professional experience mentioned on form (if applicable).
- Proof of residence if required (for application of mobility allowance).

¹ The External Staff Recruitment Application (ESRA) is the JRC's database-driven web application that manages part of the recruitment process for grantees at the JRC.

<http://recruitment.jrc.ec.europa.eu/>

- Proof of health insurance.
For Karlsruhe:
German law allows the grantholder one month to choose a public health insurance policy from the date of his/her entry into service.
For Geel/Seville:
Proof of health insurance is not required as grantholders are automatically affiliated to the Belgian/Spanish health insurance scheme.
For Petten:
Grantholders are required to apply for a Dutch health insurance within 3 months after entering the Netherlands. Grantholders who are in possession of an A1 form (or equivalent) may be exempted and continue to be covered by their previous health insurance.
- Marriage certificate and / or birth certificate of children (for application of allowances) – translations required if applicable,
- Original criminal record extract issued by the competent authority of country of origin no more than 3 months before the starting date of the grantholder contract. Should the candidate be living in a country other than his/her country of origin for more than 12 months, a further criminal record extract issued by the competent authority of this country will be required. An authenticated translation into English, French or German (or into the host language of the site) is required.
For Karlsruhe:
Extracts of criminal records are required for each country in which the candidate has lived for more than 3 months over the last 10 years. The "Sicherheitsüberprüfung" form should be filled in and signed in original for an obligatory security check carried out by the competent German authorities and required for all staff working in nuclear installations.
- Legal entity forms, bank account details (if not provided at the selection phase).
- Medical examination results sent by the candidate or by the clinic in Seville in a closed envelope marked CONFIDENTIAL are sent to the Medical Services responsible for verifying the fitness to work and confirming via a medical aptitude certificate to the RMUs/RTU (For Ispra/Seville: the Medical Service is based in Ispra. For Petten/Geel/Karlsruhe, the Medical Service is based in Luxembourg).
- Request form for reimbursement of medical expenses (except for Seville).
- Request for security opinion and, if applicable, request for derogation based on nationality for non-EU applicants.
- Request for "Nulla Osta" for EU applicants (except Karlsruhe).
- Request to national authorities for visa for non-EU applicants.

For ISPRA

- Request for Codice Fiscale – a tax identification code (if applicable).
- Accommodation form (if applicable).

For PETTEN

- A copy of the candidate's passport or ID card is transmitted to the Ministry of Finance – Dutch Tax Administration (<http://www.bekastingdienst.nl/english/>) before arrival of the grantholder. This information is not retained by the JRC.
- A copy of the candidate's passport or ID card and other personal information as requested on (<http://www.minbuza.nl/protocol>) are transmitted to the Ministry of Foreign Affairs upon arrival of the grantholder. This information is not retained by the JRC.
- Request for a BSN-SOF² number – tax identification number (if applicable).

For SEVILLE

- Support provided to non-EU candidates re their request to the national authorities for visa and work permit.

At the management phase (post-recruitment)

Includes the management of registration of contracts, payment of salaries, holidays, leave (sickness, special, parental, study...) in collaboration with the consultancy companies, teleworking requests, issuing of official working activity certificates in conjunction with the consultancy company (for Seville) and purchasing of private health insurance (if necessary). The data concerning grantholders who enter into service are collated in an Excel worksheet, which is intended for use by authorised staff of the RMUs and RTU for the Ispra site.

² BSN – Burgerservicenummer and SOFI – Sociaal Fiscaalnummer.

3. Recipients of the data

At the selection phase:

Applications for the open call for grantees are collected via the JRC web application – ESRA. The RMUs/RTU and Institute Scientific Committee members have password-protected access (ECAS) to all data in ESRA relating to their Institute via an administration module. The requesting service also has access, but only to the applications resulting from the publication of its published profile(s). An assessment report/evaluation grid ranking applicants is produced by the Selection Committee (http://ec.europa.eu/dgs/jrc/downloads/jrc_grantholder_rules.pdf). Interviews are optional. The Director of the Institute authorises the recruitment process.

At the recruitment phase:

The Unit Heads and authorised staff of the RMUs/RTU have access to the files. Internal recipients of the data include the JRC Ispra Security Service, the local security services on the non-Ispra sites, the Medical Services (based in Ispra and Luxembourg), the JRC Welcome Desk in Ispra (or the equivalent service on the other non-Ispra sites), OIB – Ispra, Finance and Procurement Unit (JRC.B.5) and the SYSPER2 Helpdesk (JRC.B.2). External recipients of the data include the German competent authority for security checks (for Karlsruhe), the national and local authorities, the company in charge of work related-risks (for Seville) and the legal consultancy companies (in charge of the preparation of monthly payments and contributions to social security).

4. Protection and safeguarding of information

ESRA is a data-base driven web application that comprises a user module (online application form) and an administration module.

Access to the user module

Data is collected online using a http connection. Data is accessed by the user (data subject) using a unique code and e-mail combination. The unique code of 12 characters is generated by a procedure combining random numbers with characters extracted from the name and surname of the user plus the application id.

Access to the administration module

Access by internal JRC users is regulated by ECAS³. The recruitment files are electronically stored on the servers located in the JRC Data Centre. These servers and associated data and operations comply with JRC security decisions and provisions (DPO-1946 on ICT Infrastructure at the JRC). Paper documents are archived in physical files, which are stored in the archives of the RMUs and the RTU (for Ispra) and are only accessible to those authorised.

5. Verification, modification and deletion of personal data

It is the responsibility of the data subject to ensure that the information provided is accurate.

At the application phase before the application is finalised:

The data subject can edit his/her application at any time before its finalisation in ESRA. Once the data subject has decided to electronically submit his/her application, changing and adding data is no longer possible. After the deadline for submission of the electronic application, the data subject has no possibility to access his/her online data.

After the application is finalised:

In case there is a need for a data subject to verify the personal data stored on his/her behalf by the controller or if there is a need for the data to be modified, deleted or the application to be withdrawn, an e-mail message should be sent to the following functional mailbox address: jrc-recruitment-data-protection@ec.europa.eu

Data subjects can gain access to their assessment report/evaluation grid from the selection phase. Access will not be granted to comparative data concerning other applicants (comparative results) nor to the individual opinions of the members of the selection panel if such access would undermine the

³ ECAS is the European Commission Authentication Service that enables web applications to authenticate centrally with a common strong password.

rights of other applicants or the freedom of the selection panel members. Requests submitted by the data subjects shall be evaluated on a case-by-case basis. Where acceptable, the relevant actions will be taken within 14 days from the date of the request.

6. Retention of personal data

Selection and recruitment files for grantholders are preserved in accordance with national law for 'n years'⁴. For files linked to unsuccessful candidates, those refusing a position or cancellation of a call, retention is for a period of 2 years after the date of entry into service of the chosen candidate. Data in SYSPER2 are retained in accordance with its retention policy. In exceptional circumstances such as a case pending before the Court, the preservation of data for longer than that which is prescribed by national law would be justified by the JRC.

7. Contact Information

For questions related to the processing of personal data an email should be sent to the functional mailbox of the Controller:

- jrc-recruitment-data-protection@ec.europa.eu

For questions relating to the protection of personal data, contact can be taken with the:

- Data Protection Co-ordinator of the JRC:
jrc-data-protection-coordinator@ec.europa.eu
- Data Protection Officer of the European Commission:
data-protection-officer@ec.europa.eu

8. Appeals

In the event of a dispute, a complaint can be sent to:

- European Data Protection Supervisor:
edps@edps.europa.eu

⁴ For Belgium, n = 5 years after the termination of the contract.
For Germany, n = 10 years after the termination of the contract taken to the end of that calendar year.
For Italy, n = 10 years after the termination of the contract.
For the Netherlands, n = 10 years after the termination of the contract.
For Spain, n = 4 years after the termination of the contract.