



EUROPEAN COMMISSION  
JOINT RESEARCH CENTRE

Resources  
Recruitment and Training Unit

February 2012

## MANAGEMENT OF SELECTION AND RECRUITMENT FILES FOR TRAINEES AT THE JOINT RESEARCH CENTRE Privacy Statement

### 1. Identity of the controller

Personal data supplied by candidates as part of a selection and recruitment procedure for trainees 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 (JRC) represented in this case by the Director of Resource Management. The Head of the Recruitment and Training Unit (RTU) for Ispra and the Heads of the Resource Management Units (RMUs) of the Institutes 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 trainees for Ispra, Geel, Karlsruhe and Petten. Seville and Brussels are excluded.

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

A traineeship file contains all the information pertaining to the selection and recruitment of trainees, which involves the RTU and RMUs, the requesting service and the potential trainees. The traineeship process commences with the launch of a call published on the JRC internet website(s) and covers the selection process (managed by the RTU and RMUs) and the recruitment procedure covering the finalisation of the trainee file (managed by the RTU for Ispra and the RMUs for the other sites).

At the selection phase (via the JRC web application tool - ESRA<sup>1</sup>):

Basic personal data are collected such as surname, name, address, contact telephone numbers, e-mail address, gender, nationality, place/country of birth, date of birth and place of recruitment. Other additional information gathered relates to university education, languages and previous work experience (if applicable), a Curriculum Vitae and a motivation letter.

At the recruitment phase:

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

- Updated Curriculum Vitae.
- Copy of passport or ID card.
- 2 passport photos.
- Medical documents and reimbursement of medical expenses (where applicable).

The Medical Service processes data relating to the health of the future trainee.

- For Petten/Geel/Karlsruhe:

The Medical Service in Luxembourg receives the medical test results from the trainee via post and verifies the fitness to work and confirms via a medical aptitude certificate to the RMUs.

- For Ispra:

For trainees with a contract of fewer than 6 months, the Medical Service in Ispra receives the medical test results from the trainee via post and verifies the fitness to work and confirms via a medical aptitude certificate to either the RTU or RMUs.

- Health card/or insurance valid in country of JRC site.
- Original criminal record extract (executed within the preceding 3 months of the starting date of the traineeship) issued by the competent authorities of country of origin. Should

---

<sup>1</sup> External Staff Recruitment Application.

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 authorities of this country will be required. An authenticated translation into English, French or German (or into the host language) 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*

*"Sicherheitsüberprüfung" form, which 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.*

- Request for Nulla Osta for all EU applicants (except Karlsruhe) and request for security opinion, derogation and Nulla Osta for non-EU applicants.
- Depending on the type of the traineeship:
  - If Type 1 - Proof of the applicant's university registration and/or a letter from the applicant's supervising professor indicating the title of the thesis.
  - If Type 2 - Copy of university degree, Master's degree or Ph.D.
  - If Type 3 - Proof of the requirement for an industrial placement.
- Proof of language skills.
- Legal Entity form and Bank Account information.
- Trainees receiving a scholarship from a bona-fide institution must declare the amount to the JRC (Art. 6.1.2 of the "Rules governing the traineeship scheme of the JRC") by providing proof of such.
- *Accommodation form (for Ispra only).*
- *For Petten, 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 trainee. This information is not retained by the JRC.*

The data concerning all the trainees who enter into service are collated in an Excel worksheet, which is intended for use by authorised staff in the RTU and RMUs.

### **3. Recipients of the data**

At the selection phase:

Applications for the open call for trainees are collected via the JRC web application – ESRA. The RTU and RMUs have password-protected access (ECAS) to all data in ESRA relating to their Institute/Directorate via an administration module<sup>2</sup>. 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 requesting service and forwarded to the RTU/RMUs for follow-up. The Director of the Institute/Directorate authorises the recruitment process.

At the recruitment phase:

The Unit Heads and authorised staff of the RTU/RMUs have access to the files.

Other recipients of the data include the JRC Ispra Security Service, the local security services on the non-Ispra sites, the German competent authority for security checks (for Karlsruhe), the Medical Services (DG HR based in Ispra and Luxembourg), the JRC Welcome Desk based in Ispra (or equivalent service on the other sites), the OIB for Ispra, the Finance and Procurement Unit (JRC.B.5) and the SYSPER2 Helpdesk (JRC.B.2).

### **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.

---

<sup>2</sup> The Human Resources unit acts as administrator for the administration module.

Access to the administration module

Access by internal JRC users is regulated by ECAS. ECAS is the European Commission Authentication Service that enables web applications to authenticate centrally with a common strong password.

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 RTU/RMUs 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 all 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](mailto:jrc-recruitment-data-protection@ec.europa.eu). Data subjects can gain access to their assessment report/evaluation grid from the selection phase. They can be provided with the aggregated results of the selection phase (although they will have no access to information about other data subjects involved in the selection procedure). 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**

In accordance with Commission SEC(2007)970 of 4 July 2007, personal files for recruited trainees are classified and stored for a period of 50 years with elimination after five years of all documents except the online application forms, offers of traineeships, letters of acceptance and attestations of traineeships. Files on candidates who are a) rejected; b) not pre-selected; c) pre-selected but not recruited; or d) who withdraw their application are retained for 2 years after the date of entry into service of the recruited trainee. These files contain candidates' applications and related correspondence. Data in SYSPER2 are retained in accordance with the retention policy of SYSPER2. In exceptional circumstances such as a case pending before the Court, the conservation of data 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](mailto: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](mailto:jrc-data-protection-coordinator@ec.europa.eu)
- Data Protection Officer of the European Commission:  
[data-protection-officer@ec.europa.eu](mailto: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](mailto:edps@edps.europa.eu)