

SELECTION/RECRUITMENT PROCEDURE FOR CONTRACT STAFF MEMBERS 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 contract staff (FG I) and auxiliary contract staff (FG II, III and IV) – collectively grouped as contract staff members – are 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 Resources. The Head of the Recruitment and Training Unit (RTU) and the Heads of the Resource Management Units (RMUs) of the JRC are responsible for internally managing the processing operation on behalf of the controller.

The legal basis of the processing operations for the recruitment of contract staff derives from Article 79 of the Conditions of Employment of Other Servants of the EU (CEOS). The Commission Decision of 2.3.2011 on the general provisions for implementing Article 79(2) of the CEOS govern the conditions of employment of contract staff employed by the Commission under the terms of Articles 3a and 3b of the said Conditions. The information requested in relation to possible conflicts of interest is based on Article 81 of the CEOS.

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

The main purpose of the collection of the data is to prepare the selected candidate's file and to finalise the recruitment procedure involving the preparation of the grading and entry into service permit.

Summary of procedure for recruitment of Contract Staff members (FGI-IV):

1. Selection in CAST database (access provided by RTU and RMUs) by JRC recruiting unit.
2. Organisation of interviews with evaluation sheets being compiled for all candidates.
3. File preparation by RTU and RMUs.
4. File constitution and verification by the RTU (for Ispra/Brussels) or by the RMU on the other sites.
5. File finalisation by RTU (for Ispra/Brussels) or the RMUs on the other sites.

At the selection phase

Invitation to interview letter:

- The preparation of the permit to enter the site requires a copy of the candidate's passport/identity card. For Petten, all candidates must identify themselves with a passport/identity card or any other official identification document mentioning their nationality. For Karlsruhe, the entry permit is done in parallel with the decision on reliability screening (see below). For Seville, the entry permit is prepared upon arrival of the candidate and upon presentation of his/her original passport/identity card.
- The reimbursement of travel and/or accommodation expenses (if applicable) requires that the candidate supply a financial identification and a legal entity form with a copy of his/her passport/identity card and a bank stamp and signature on the financial identification form (a bank account extract is possible as a substitute). The request for reimbursement form must be compiled and travel receipts attached.

At the recruitment phase:

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

Personal data:

- name, surname, date of birth, nationality, civil status, private address

Documents collated

- conflict of interest form to be filled in by the candidate and signed by the hierarchy of the recruiting service;
- original criminal records extract(s) from the national database of your latest country of residence. Should you be resident in that country for less than 6 months, a valid and original criminal record extract emanating from your previous country of residence where you have been living for at least 6 months is required. The criminal record extract should be in one of the 24 official languages of the European Union. A translation into English, French, German or the language of the country in which the JRC site is located is recommended in order to speed up our procedures. If the criminal record extract is issued in a language other than the 24 official languages of the European Union, a legalised translation into English, French, German or the language of the country in which the JRC site is located is required. The criminal record extract is assessed on a case-by-case basis in order to collect only the relevant information in light of the requirement of the Staff Regulations and Conditions of Employment of Other Servants of the European Union.
- application form + professional experience form
- updated curriculum vitae
- birth certificate
- marriage certificate and/or divorce or legal separation judgments, and/or official declaration of partnership recognition – if applicable
- birth certificate(s) of child(ren) – if applicable
- declaration of spouse's/partner's professional income, declaration of eventual family allowances from other sources – if applicable
- passport/ID card (if not previously provided at an earlier stage)
- document proving the fulfillment of any military obligations
- diploma giving access to relevant Function Group
- other relevant diplomas
- previous work contracts or work certificates and/or salary slips and/or tax declarations
- entry VISA for non-EU citizens (if applicable)
- Legal Entity form (if not already provided)
- Reimbursement of travel and subsistence expenses form (if applicable)
- Medical aptitude certificate (the Medical Services are responsible for verifying the fitness to work. For Ispra/Seville, the Medical Service is in Ispra; for Petten/Geel/Karlsruhe, the Medical Service is in Luxembourg and for Brussels, the Medical Service is in Brussels).

Only for Karlsruhe site:

- an original criminal record extract for each country in which they lived for more than 6 months over the last 10 years
- a "Sicherheitsüberprüfung" form, filled in and signed in original for an obligatory security check, which will be carried out by the competent German authorities (the information is communication to the authorities in a sealed envelope). This requirement is applicable to all staff working in nuclear installations (Zuverlässigkeitsprüfung).

3. Who has access to your information and to whom is it disclosed?

The RMUs and RTU and corresponding file managers have full access to recruitment files and related information. Monitoring tables are retained by RMUs/RTU for expiry dates and renewals. The last step of the recruitment procedure is to inform the Directorates, SYSPER2, the Security Service, the Medical Services, OIB, PMO of the candidate's entry into service. For Karlsruhe, the competent German authority is involved. In addition, IDOC is informed in case of doubt regarding a candidate's "criminal record extract". All recipients are reminded regularly of their obligation not to use the data received for any further purpose other than the one for which they were transmitted.

4. How do we protect and safeguard your information?

Recruitment (personal) files are electronically stored on the servers located in the JRC Data Centre. These servers and associated data and operations satisfy the JRC's security decisions and

provisions. Recruitment (personal) files are also physically archived in the HRU and the selection files are physically archived by RTU for Ispra/Brussels and the RMUs on the other sites.

5. How can you verify, modify or delete your information?

In case you wish to verify the personal data stored on your behalf by the responsible controller, have the data modified or deleted, an e-mail message should be sent to the following functional mailbox: jrc-recruitment-data-protection@ec.europa.eu

Data subjects (both selected and non-selected candidates) can gain access (although this does not grant any rectification rights) to their assessment report/evaluation grid from the selection phase. The right of access is different from that of the right of rectification. The right of access enables the candidate to see if the selection process was carried out fairly and objectively. Please take note that 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 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.

Personal data of recruited candidates are stored in Sysper2 and NDP, which may be consulted at any time as provided for in Article 92 of the "Conditions of employment of other servants of the European Communities" which shall apply by analogy Article 26, paragraph 7 of the "Staff Regulations of Officials of the European Communities".

Requests (addressed to the functional mailbox) submitted by a candidate shall be evaluated and where acceptable, the relevant actions will be taken within 14 days from the date of the request. In exceptional circumstances (e.g., in the case of an ongoing litigation), the data will be retained for longer.

6. For how long do we keep your data?

Selection files on paper are stored for a period of 5 years from the date of entry into service of the successful candidate in accordance with SEC(2012)713 of 17 December 2012. For the recruitment files a defined portion of the file is transferred to the individual's personal dossier (NDP) and retained in accordance with the obligations outlined in SEC(2012)713 of 17 December 2012: 8 years after the extinction of all rights of the person concerned and of any dependants and at least 120 years after the date of birth of the person concerned.

Salary slips (when no work contracts/work certificates are available) for grading purposes (if requested) are stored for a maximum period of 2 years from the date of entry into service of the successful candidate and are then eliminated. Criminal record extracts are stored for up to two years from the date of recruitment; records that have been checked by the Court of Auditors before the end of this period can be destroyed earlier.

For candidates declining the offer and for cases where the position is cancelled in the interests of the service, the files are retained for a period of 2 years and then eliminated.

7. Contact Information

For questions related to the processing of personal data an email should be forwarded 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