



European Economic
and Social Committee

**Record of processing activity
Part 1**

Name of the data processing

Created on

Last update

Reference number

Year

1. Controller: European Economic and Social Committee

2.a) Service responsible

2b) contact details
Directorate for Human Resources and Finance, European Economic and Social Committee (recrutement-carriere@eesc.europa.eu)

3. Joint controller
Not applicable

4. DPO: contact details data.protection@eesc.europa.eu

5. Processor(s) (where applicable)
Not applicable

6. Purpose(s) of the data processing

Article 5 of the CEOS defines "special adviser" as "a person who, by reason of his special qualifications and notwithstanding gainful employment in some other capacity, is engaged to assist one of the institutions of the Union, either regularly or for a specified period". In this context, the EESC may recruit a special adviser with functions of medical adviser. To this end, the EESC collects, manages and stores data relating to candidates who apply for these functions. Following publication of the vacant position, applications are collected by means of an *ad hoc* online application tool, known as "Microsoft Dynamics CRM. The purpose of processing personal data submitted via this online tool is to efficiently collect applications addressed to the EESC and recruit the candidate who presents the most suitable profile. It ensures secure collection of data submitted by the applicants and therefore facilitates the work of the EESC recruitment services. It also serves the purpose of verifying the eligibility of applicants.

7. Description of the categories of persons whose data are processed

candidates who have applied to the vacant position via the online application tool, from various sources external to the EU institutions, bodies or agencies.

8. Description of data categories processed

For the selection phase : data identifying the applicant such as name, first name, nationality, gender, date and place of birth, postal and e-mail address, telephone number and, if necessary (very rare), a statement declaring any disability. Documents requested to verify whether the application is admissible or not: a curriculum vitae, a covering letter, a certificate proving the applicant's status as medical doctor. On their own initiative, applicants may send other information such as letters of recommendation, certificates showing language competences, etc.

For the recruitment phase : police record, diplomas, certificates of previous employment experience, training, and data required for the payment of salary: data concerning the identity of the person concerned, financial information forms (legal entity and bank identification), declaration of absence of conflict of interest.

9. Time limit for retaining the data

Data related to the selection process, including data from candidates who have not been retained, are kept by the Recruitment sector of Unit PER **for 3 years**, starting from the date of effect of the contract of engagement (this period is justified for auditing purposes)

In case of legal action against the engagement decision, the retention period is extended until one year after the final decision.

The electronic data of candidates who have not been retained, consisting of CV, supporting documents, copies of diplomas will be destroyed **after 3 years**. The names of all candidates, including of those who have been excluded at some point of the process, remain on the minutes recording the conclusions of the selection panel, for statistical and historical records. These minutes, as data related to the selection process, are also kept for a duration of 3 years and then destroyed.

Data related to the recruited applicant are kept **10 years** after the end of his engagement contract. The relevant documents related to his eligibility are kept in his individual file. Documents related to a potential request linked to a handicap are destroyed after the closure of the selection process, unless expenses have been incurred by this request : in such case, these documents will be destroyed after 3 years (this duration is justified for auditing purposes).

When the retention period has expired, the documents are destroyed.

10. Recipients of the data

For the selection phase :

- Hierarchical superior in charge of the entity where the vacant position was published for the pre-selection and selection phases.
- the members of the selection board
- the HR members in the Recruitment sector (REC) of unit PER
- only in case of technical problems, the "Dynamics" team of Unit "Online Information (INF)" offering technical support to users on the unit "Information technologies and telecommunication (ITT)" as system administrator of online application tool

For the recruitment phase :

- the HR members in the Recruitment sector (REC) of unit PER
- the Communication and administrative documents sector (ADI)
- the Financial verification sector
- the Salary sector
- the Rights and Obligations sector
- the Appointing Authority or its delegate

11. Transfers of personal data to a third country or an international organisation

There is no transfer of personal data to third countries or international organisations .

12. General description of security measures, where possible

Applications for a vacancy are available electronically by the Recruitment sector as processing entity via the tool "Dynamics", separately for each individual vacancy/selection procedure) and, if considered necessary by the processing entity, it may also be printed (for the pre-selection or selection panel members) and stored physically (on paper).

Physical storage (paper archives): if printed by the processing entity for the purpose of selection panel meetings, applications will afterwards be stored in locked cupboards or in a cupboard in a locked room. The hierarchical superior of the entity where the vacancy was published and all the panel members will be reminded to destroy any paper files or emails containing personal data once the selection procedure is finalised and the selected candidate is appointed. They will be asked to sign a specific form to this end (the declaration of confidentiality). The paper files are stored only by the processing entity and they will be destroyed 3 years after the end of the selection procedure, starting from the date of taking up duties by the recruited candidate.

13. Privacy statement

[recruitment medical adviser](#)

Part 2 Compliance check and risk screening

1.a) Legal basis and reason for processing

- necessary for the performance of a task carried out in the public interest
- (a) or in the exercise of official authority vested in the Union institution or body
- (b) necessary for compliance with a legal obligation to which the controller is subject (see point 1b) below)
- processing is necessary for the performance of a contract to which the
- (c) data subject is party or in order to take steps at the request of the data subject prior to entering into a contract
- (d) the data subject has given consent to the processing of his or her personal data for one or more specific purposes
- (e) necessary in order to protect the vital interests of the data subject or of another natural person

[Tick (at least) one of the boxes]

1b) Legal basis

The legal basis for the processing operation is Article 124 of the CEOS, referring in particular to Article 23 of the EU Staff Regulations on the rights and obligations of officials, applicable by analogy.

2. Are the purposes specified, explicit and legitimate?

Yes

3. Where information is also processed for other purposes, are you sure that these are not incompatible with the initial purpose(s)?

Yes

4. Do you really need all the data items you plan to collect?

Yes all data collected is needed.

| | |
|--|--|
| 5. How do you ensure that the information you process is accurate? | Supporting evidence such as ID, diplomas, certificates of professional experience, certificates of training, extract of police record must be presented by the candidates. |
| 6. How do you rectify inaccurate information? | Based on supporting evidence, candidates may address any request of rectification to the data controller. |
| 7. Are they limited according to the maxim "as long as necessary, as short as possible"? | Yes |
| 8. If you need to store certain information for longer, can you split the storage periods? | Not in the case of electronic storage, but feasible in the case of paper storage. |
| 9 How do you inform data subjects? | By way of a specific privacy / confidentiality statement available via the hyperlink, as part of the vacancy notice, or the financial forms, or in exchange of emails. |
| 10. Access and other rights of persons whose data are processed | Requests from data subjects, regarding access, deletion, correction of data addressed to the data controller are followed up within 15 days of introducing the request. |
| 11. Does this process involve any of the following? | <input type="checkbox"/> (a) data relating to health, (suspected) criminal offences or other special categories of personal data <input type="checkbox"/> (b) evaluation, automated decision-making or profiling <input type="checkbox"/> (c) monitoring data subjects <input type="checkbox"/> (d) new technologies that may be considered intrusive |
| Part 3 Linked documentation | |
| 1. Links to threshold assessment and DPIA (where applicable) |  No hyperlink inserted |
| 2. Where are your information security measures documented? |  No hyperlink inserted |
| 3. Links to other documentation |  No hyperlink inserted |
| 4. Other relevant documents | |
| | |