

Cedefop record of processing activity

Record of Cedefop activities processing personal data, based on Article 31 of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No. 45/2001 and Decision 1247/2002/EC.

| Nr. | Item | Description |
|--|---|---|
| Selection and recruitment of Temporary Agents (TAs) and Contract agents (CAs) | | |
| 1. | Last update of this record | 14/11/2022 |
| 2. | Reference number | Case no 2009-122 – Selection and recruitment of Temporary Agents (TAs) and Contract agents (CAs) |
| 3. | Name and contact details of controller | <p>Cedefop – European Centre for the Development of Vocational Training Postal address: Cedefop, Europe 123, Service Post, 570 01 Thessaloniki, GREECE Telephone: (+30) 2310-490111 Email: info@cedefop.europa.eu</p> <p>Responsible department or role: DRS / Human Resources</p> <p>Controller contact information for enquiries on processing of personal data: hr_data_protection@cedefop.europa.eu</p> |
| 4. | Name and contact details of DPO | data-protection-officer@cedefop.europa.eu |
| 5. | Name and contact details of joint controller (where applicable) | N/A |
| 6. | Name and contact details of processor (where applicable) | <ul style="list-style-type: none"> The external service provider Oleeo Plc (https://www.oleeo.com/), on behalf of Cedefop and under specific contract, provides the software as a service platform used for the online application platform. Oleeo Privacy Statement; External contractor that may support Cedefop in different phases of recruitment and selection procedures; |

| | | |
|----|---|--|
| | | <ul style="list-style-type: none"> In case of tests or interviews conducted remotely, Cedefop uses the MS Teams conferencing platform. For further information about the processing of personal data with MS Teams, please see record of processing activity CDFNOT088 Voice-video calling and instant messaging using MS Teams. |
| 7. | Short description and purpose of the processing | <p>The data processing facilitates the organisation and management of selection and recruitment procedures of Temporary Agents (TAs) and Contract Agents (CAs) in view of filling vacancies and establishing reserve lists for future recruitments at Cedefop. It supports the management of applications at all stages of the procedure, the work of selection boards and also any appeals or legal challenges that might follow a procedure.</p> <p>During the application process, candidates create an account in Oleoo. Through this account, they manage their own contact details, and can view status, communications, and details of the Cedefop vacancies they applied to.</p> <p>Cedefop HR assistant extracts the names of applicants for a specific vacancy so that selection board members can check if they know any of them and fill in their declarations of interest. Once this step is completed, selection board members are given access to applications in Oleoo to proceed with the selection process.</p> <p>Cedefop's HR makes eligibility check (Y/N) and only those candidates who fulfil all criteria proceed to the pre-selection phase. The selection board is responsible to confirm the eligibility check.</p> <p>The selection board evaluates applications based on the pre-selection criteria (essential and other) set in the vacancy notice. The candidates that meet all essential criteria and received highest marks for the other pre-selection criteria (indicative number of candidates specified in each vacancy notice) are invited to participate in the selection phase of the process (e.g. tests, interviews). Once the selection phase is completed, the selection board prepares a selection report with a summary of the whole process and the names of candidates to be included in the list of suitable candidates. Cedefop's Executive Director receives the report and signs the list of suitable candidates.</p> <p>The legal basis for the selection procedures are the Staff regulations and the Conditions of Employment of Other Servants of the EU (CEOS), as well as their implementing provisions (Cedefop/DGE/23/2015 and Cedefop/DGE/40/2019).</p> |

| | | |
|----|---|---|
| | | <p>The lawfulness of the processing is defined by Article 5 (a) of Regulation 2018/1725 in that “processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body” and Article 5 (d) in that applicants give consent to the processing of their personal data.</p> |
| 8. | Description of categories of persons whose data Cedefop processes and list of data categories | <p>Any person who applies, for a position of Temporary Agent or Contract Agent in response to a vacancy notice published by Cedefop.</p> <p>Oleeo account (managed by applicant)</p> <ul style="list-style-type: none"> • First Name • Last Name • Email address • Password • My Vacancies <p>Application process:</p> <ul style="list-style-type: none"> • Identification and contact information: name, surname, mobile number, email address, etc; • Nationality; • Date of birth; • Education (degree name, date, name and country of awarding body); • Knowledge of languages; • Work experience (dates, job title, description, employer) • Traineeships (dates, job title, description, employer) • Pre-selection essential and other criteria for each specific vacancy (depends on each vacancy); • Motivation; • Information on military service; • Agreement on declaration of honour regarding truthful information, undergo necessary recruitment steps and consent for the storage of personal details according with Cedefop’s records management retention schedule; • In specific cases, copies or articles/papers produced by the candidate may be requested to be uploaded together their online application. |

| | | |
|----|---------------------------------|---|
| | | <p>Eligibility phase</p> <ul style="list-style-type: none"> • Application complies with eligibility criteria (YES/NO) <p>Pre-selection phase</p> <ul style="list-style-type: none"> • Application complies with essential pre-selection criteria (YES/NO) • Application complies with other pre-selection criteria (score) <p>Selection phase</p> <ul style="list-style-type: none"> • Written tests (where candidates are only identified with a unique code) • Selection report: includes test scores, selection board comments and summary of interview responses for each candidate who goes through the selection phase <p>Pre-recruitment documents requested from candidates who are invited to selection phase (test, interview)</p> <ul style="list-style-type: none"> • Criminal record • Proof of nationality (passport / national ID) • Copies of diplomas or certificates • Employment evidence (e.g. work certificates, contracts, payslips, tax declaration etc.) <p>Special Categories / Sensitive data: application data processed, and pre-recruitment documents could include data specified in the Article 10(1) of Regulation (EU) No 2018/1725 (i.e. data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs and data concerning health or sex life or sexual orientation). Special categories of data will be stored securely in encrypted form.</p> |
| 9. | Time limit for keeping the data | <ul style="list-style-type: none"> • data of the recruited applicants will be stored in the personal file and related retention schedule for personal files will apply (see record CDFNOT037 Personal files); • pre-recruitment documents of candidates on a list of suitable candidates will be kept for 3 years after the expiry date of the list; • data of the applicants who were preselected but not subsequently included on a list of suitable candidates will be kept for 3 years after the related selection process is finished; • data of the applicants who were not preselected is kept for 2 years after the related selection process is finished. |

| | | |
|-----|---|---|
| | | <ul style="list-style-type: none"> Oleeo system: In the absence of a specific written data retention agreement, Oleeo will retain Candidate data for 12 months following the closure of the deadline for submission of applications (Oleeo – CEDEFOP agreement, Schedule 7 – Security Requirements). |
| 10. | Recipients of the data | <p>Internal recipients:</p> <ul style="list-style-type: none"> the staff in the HR service responsible for the selection procedures have access to all personal data; the members, advisors and/or observers of the selection board (internal or external) appointed by the Executive Director have access to personal data of submitted applicants using the Oleeo application; Cedefop’s Executive Director (if necessary); designated Cedefop ICT administrators with access to the Oleeo application; the legal function of Cedefop (if necessary) the appeals committee (if necessary); <p>External recipients:</p> <ul style="list-style-type: none"> Oleeo Plc staff may have access to the data in order to provide technical support to candidates and/or Cedefop staff. designated staff of the company contracted to give support to the selection board for a given selection procedure (if necessary); the Commission and MB representatives (this would only apply to the selection of the Executive Director and Deputy Director); external lawyers contracted to provide advice/assistance with issues concerning specific selection cases/procedure (if necessary); the Court of Auditors, Cedefop’s ICC, the Internal Audit Service of the Commission, the European Ombudsman, the Civil Service Tribunal and the European Court of Justice may also have access, as may lawyers contracted, in connection with a selection-related lawsuit. |
| 11. | Are there any transfers of personal data to third countries or international organisations? If so, to which ones and with which safeguards? | <p>Any personal data collected through our online application system is stored in Oleeo’s certified data centres within the UK. More information about how the personal data are processed by Oleeo may be found here.</p> <p>Safeguards:</p> <ul style="list-style-type: none"> UK GDPR considered essentially equivalent to GDPR; Standard Contractual Clauses (Oleeo – CEDEFOP agreement, Schedule 9 – Data Processing). |

| | | |
|-----|--|--|
| 12. | General description of security measures where possible. | <ul style="list-style-type: none"> • HR is responsible for the storage electronic and/or paper files. For the latter, there are secure areas such as locked cabinets and the Archive room. HR is also responsible for the destruction of those files as per the records management retention schedule; • Applications received and supporting documents to be treated as sensitive, non-classified (SNC) data¹; • SNC data is encrypted (DKE to be used for Special categories of data); • Cedefop networks and ICT systems (e.g. records bank) follow Cedefop's ICT Security policy (e.g. authentication, role-based permissions, etc.); • Electronic documents stored in Cedefop's M365 Sharepoint online environment are encrypted both at rest and in transit; • Confidentiality awareness; • Communication of data is restricted to those persons who "need to know" for the performance of their duties. <p>Oleeo security measures:</p> <ul style="list-style-type: none"> • SSL protocol; • use of password and Captcha; • lock of account after three unsuccessful login attempts; • Oleeo will engage a 3rd party on an annual basis to conduct both a host based and application-based security assessment of the System. If the Client wishes at any point to conduct its own security review it may do so. • Oleeo commits itself to implement measures to allow the processing of Personal Data and other information received separately from different customers, ensuring that at each step of the processing the controller can be identified • Oleeo shall, in relation to the Client Personal Data, implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, which may include: <ul style="list-style-type: none"> ○ the pseudonymisation and encryption of Personal Data; ○ the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; |
|-----|--|--|

¹ RB(2019)01250 DIR decision - Rules on sensitive non-classified information

| | | |
|-----|---|---|
| | | <ul style="list-style-type: none"> ○ the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; ○ a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing; ○ reasonable measures to protect personal data from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed; • access to the application operations is managed through the definition of roles and the respective assignment to users; • the public and the back-office parts of the application are split in order to prevent access to sensitive data from the public site. |
| 13. | For more information, including how to exercise own rights to access, rectification, object and data portability (where applicable), see the privacy statement: | Privacy statement linked to vacancy application form |