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
	Learning and Development training records	
1.	Last update of this record	19/09/2025
2.	Reference number	RB2025-1948425193-2515
3.	Name and contact details of controller	Cedefop – European Centre for the Development of Vocational Training **Postal address:** Cedefop Service Post, Europe 123, 570 01 Thermi, GREECE **Telephone:** (+30) 2310 490111 **Email:** info@cedefop.europa.eu Responsible department or role: The responsible department is Department for Resources and Support, and the responsible service is Human Resources Service. Contact form for enquiries on processing of personal data to be preferably used: hr_data_protection@cedefop.europa.eu
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)	Cedefop's contractors providing various Learning and Development sessions e.g. trainings, online talks, workshops,team building activities etc.
7.	Very short description and purpose of the processing	The purpose of the processing is to identify, organise and manage learning and development activities to Cedefop staff members (Officials, Temporary Agents, Contract Agents), Seconded National Experts, trainees and interims approved by the Head of Departments, Reporting Officer(s), Reporting Officers by delegation and/or Supervisor(s) for talent development to facilitate access and keep track of activities to ensure proper functioning of the service. The legal basis of the procedure is: The processing of personal data is necessary for the performance of tasks carried out in the public interest and for compliance with a legal obligation to which Cedefop is subject, as per Article 5(1)(a) of Regulation (EU) 2018/1725. **Specific Legal Bases:** • Article 5(1)(d) of Regulation (EU) 2018/1725 • Staff Regulations art. 24a • Staff Regulations of Officials and Conditions of Employment of Other Servants of the European Union (CEOS) art. 11 and 81 • Staff Regulations art. 45.2 of the of Officials • CEOS art. 85(3) • Cedefop/DGE/39/2019 (general implementing provisions on learning and development).
8.	Description of categories of persons whose data Cedefop processes and list of data categories	Cedefop staff members (Officials, Temporary Agents, Contract Agents), Seconded National Experts, trainees and interims approved by the Head of Departments, Reporting Officer(s) and/or Reporting Officer by delegation and/or Supervisor(s). Personal Data processed per category:

		• **Identification data:** name, surname, department, job title of staff member, reporting officer, reporting officer by delegation, Learning and Development Officer, gender, course details • **Contact data:** e-mail of staff member and/or reporting officer, reporting officer by delegation, Learning and Development Officer • **Other information:** level of knowledge, expectations, post-training feedback on quality of training/session, request reasoning • **Photo, videos, bios, meeting recordings and chat** • **Introducing new staff:** role, background, hobbies, photo
9.	Time limit for keeping the data	The time-limits for storing personal data are as follows: • **individual training file:** for 2 years after a staff member leaves Cedefop • **courses records:** including participant list, evaluation of the course, a summary of the evaluations, and all related correspondence for 5 years after the related contract expires • **information of courses records:** for 2 years after the information has been superseded or has become obsolete • **staff training plan:** for 2 years
10.	Recipients of the data	Cedefop's staff internally responsible for audit and review activities, as well as staff of external contractors providing audit and review services to Cedefop, may have access to the personal data collected through this processing operation to the extent necessary for carrying out their activities. <u>Internal recipients</u> • The L&D Officer, and HR staff member who supports the L&D Officer and the Head of HR to identify learning needs and provide support; • Head of Departments and/or reporting officers (by delegation) who approve training requests; • Assistants of Head of Departments who monitor the training requests and department budget

		• Designated Cedefop ICT administrators with access to internal application tools for L&D purposes • Designated Finance and Procurement colleagues responsible for payments • List of participants with access to internal database External recipients • Data may be accessed by external auditors during audits • Staff members of other Agencies, if there is participation to joint event/training activity with other Agencies • External training providers or experts • European Commission as a provider of EU Learn and EU Survey platform provider • Microsoft • Webex • Slido • Flow Forma • Zoom
11.	Are there any transfers of personal data to third countries or international organisations? If so, to which ones and with which safeguards?	• MS Teams (Microsoft Ireland Operations Ltd.) may transfer personal data for technical support purposes to Microsoft Corporation located in the US and to the entities affiliated to it. Such transfers are based on the European Commission's adequacy decisions or Standard Contractual Clauses. Please refer to the specific privacy statement. • Slido (Cisco Systems, Inc.) may transfer personal data for technical support purposes to US and other countries based on the European Commission's adequacy decisions, Standard Contractual Clauses and/or Binding Corporate Rules. Please refer to Slido privacy statement.

		• Webex (Cisco Systems, Inc.) may transfer personal data for technical support purposes outside the European Economic Area, to US based on EU Binding Corporate Rules and EU Standard Contractual Clauses. Please refer to Cisco Webex privacy statement. • Zoom may transfer personal data for technical support, marketing, advertising and analytics purposes to California and other US states based on European Commission's Standard Contractual Clauses. Please refer to Zoom privacy statement. 1. Transfers of personal data by Slido: When Slido is used, it may transfer personal data to its staff and service providers, as well as to its parent company Cisco Systems, Inc. and Cisco's affiliates acting as sub-processors, for the purpose of providing its services. All these transfers of personal data are taking place based on Standard Contractual Clauses. 2. Transfers of personal data by Webex: Alternatively, when an external training provider is involved and uses Webex, Cisco Systems Inc. that provide Webex, may transfer personal data to Cisco in the United States of America, to any Cisco subsidiary worldwide, or to third parties and business partners worldwide. Any transfer of personal data by Cisco relies on an adequacy decision, or, in the absence of it, on Standard Contractual Clauses, Binding Corporate Rules—Controller, or other legal transfer mechanisms with appropriate safeguards in place to protect personal data. Additionally, Cisco Systems, Inc. and its U.S. based subsidiaries (collectively "Cisco-U.S.") comply with the EU-U.S. Data Privacy Framework (EU-U.S. DPF). 3. Transfers of personal data by Zoom: Alternatively, when an external training provider is involved and uses Zoom as the video-conferencing platform for the event, Zoom Video Communications, Inc. may transfer personal data outside of the EU/EEA. These data transfers take place based on an adequacy decision for the country where the data are

		transferred and stored, or, in the absence of such an adequacy decision, based on the European Commission's Standard Contractual Clauses. Specifically for data transfers to the EU, Zoom with its 3 entities complies with the EU-US Data Privacy Framework as a self-certified US-based company.
12.	General description of security measures where possible.	Cedefop implements a number of technical and organisational security measures to address, among others, online security (firewall, URL filtering, antivirus programs), risk of data loss and alteration (back-up and restore policy), as well as to grant access to its information and documents only to authorised users based on a 'need to know' principle (through authentication and authorisation procedures, encryption). Cedefop has also put in place appropriate incident handling and personal data breaches procedures. Compliance with these measures is ensured through Cedefop's ICT Use and Security Policy, which is regularly reviewed for improvements.
13.	For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	A Privacy Statement is made available to data subjects by, e.g. sending it via email, providing a link to access it. You have the right to request from the controller access to and rectification or erasure of your personal data or restriction of processing. You also have the right to object to the processing of your personal data. If you have given consent to any of the related processing activities, this can be withdrawn at any time, without undermining the lawfulness of processing undertaken until that point. To exercise the mentioned rights, you may contact the controller by sending an email to: hr_data_protection@cedefop.europa.eu. The controller shall provide information on action taken on a request within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests.

		For further inquiries, you may refer to Data Protection Officer of Cedefop (data-protection-officer@cedefop.europa.eu). Finally, if you consider your data protection rights have been breached, you may lodge a complaint with the European Data Protection Supervisor as the supervisory authority using a dedicated complaint form: https://edps.europa.eu/data-protection/our-role-supervisor/complaints_en (see further contact information at https://edps.europa.eu/about-edps/contact_en).