

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
<i>Department for VET and Skills (DVS) Stakeholder Database</i>		
1.	Last update of this record	20/08/2026
2.	Name and contact details of controller	Cedefop – European Centre for the Development of Vocational Training Postal address: Cedefop Service Post, Europe 123, 570 01 Thessaloniki, GREECE Telephone: (+30) 2310 490111 Email: info@cedefop.europa.eu <u>Responsible department or role:</u> Department for VET and Skills (DVS)
3.	Name and contact details of DPO	data-protection-officer@cedefop.europa.eu
4.	Name and contact details of joint controller (where applicable)	N/A
5.	Name and contact details of processor (where applicable)	EU Survey platform
6.	Very short description and purpose of the processing	The purpose of this processing operation is to register new stakeholders in the department's database. This database allows the Controller to communicate with contacts active in the fields of vocational education and training (VET), skills, and qualifications, and to

		manage email campaigns about activities organised by DVS and Cedefop, in support of their work, in line with the Agency's Communications Strategy. The lawfulness of the processing is defined by Article 5(1)(a), in that the processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official authority vested in the Union institution or body, and particularly, as set forth in Article 2 of the Regulation (EU) 2019/1282, since this processing operation is relevant to the functioning of the institution/agency. Additionally, the lawfulness of the processing is defined by Article 5(1)(d) of the Regulation (EU) 2018/1725. In particular, individuals must register via the EU Survey and provide their informed consent to be included in the DVS database and to be contacted in relation to one or more of the activity types provided therein.
7.	Description of categories of persons whose data Cedefop processes and list of data categories	The following personal data of stakeholders is collected: Personal Information (Mr/Ms, Name, Surname); Email; Country; Institution/organisation name and Department; Position; Type of stakeholder; Researchers/Experts; Type of network.
8.	Time limit for keeping the data	The time-limits for storing personal data are as follows: Personal data will be retained for as long as the data subject wishes to remain active in the DVS database of stakeholders, and up to a maximum of 10 years starting from the day that the personal data are included in the database, in accordance with Cedefop's Retention List. The database is regularly monitored by the responsible Information Manager, who removes records associated with invalid email addresses (e.g. bounced emails, expired domains, change of), or and information about data subjects that have withdrawn their consent.

9.	Recipients of the data	Access to your personal data is provided to Cedefop staff responsible for carrying out this processing operation and to other authorised Cedefop staff according to the “need to know” principle. Such staff abide by statutory, and when required, additional confidentiality agreements. Cedefop’s staff internally responsible for audit and review activities, as well as staff of contractors providing audit and review services to Cedefop, may access the personal data collected through this processing operation to the extent necessary for carrying out their duties.
10.	Are there any transfers of personal data to third countries or international organisations? If so, to which ones and with which safeguards?	N/A
11.	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.
12.	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 providing a link to access it.