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
	Personal Data Breaches	
1.	Last update of this record	30/09/2025
2.	Reference number	RB2025-1948425193-2528
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: Executive Director´s Office/ Data Protection Officer
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)	N/A
7.	Very short description and purpose of the processing	The purpose of the processing is to identify situations where there occurs a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted,

		stored or otherwise processed; and to secure the situation of assessing and examining the scope and severity of personal data breach and measures to be taken. Also, documenting, and, if needed, communicating the personal data breach to EDPS and/or to data subject. The legal basis for the processing activity is: Article 5(1)(b) of Regulation (EU) 2018/1725 - legal obligation under Articles 33-35 of Regulation (EU) 2018/1725; notification to the EDPS. A specific documentation for handling and notifying personal data breach is derived from this procedure: Policy and procedure for handling and notifying personal data breaches at Cedefop. The needed actions are also governed by: Procedure for handling and notifying personal data breaches.
8.	Description of categories of persons whose data Cedefop processes and list of data categories	<u>Data subjects:</u> Internal: - any individuals, whose personal data are processed by Cedefop as controller or its processors, might potentially be affected by a personal data breach. In particular, the personal data of the following data subjects may be processed: - controllers and delegate controllers of Cedefop involved in a personal data breach; - Cedefop staff who inform the Data Protection Officer of a personal data breach, and/or are involved in managing a personal data breach; External: - any individuals, whose personal data are processed by Cedefop as controller or its processors, might potentially be affected by a personal data breach. In particular, the personal data of the following data subjects may be processed: - any individual who informs the Data Protection Officer of a personal data breach;

		- responsible staff of Cedefop´s processor (if relevant) who inform the Data Protection Officer of a personal data breach, and/or are involved in managing the personal data breach; - EDPS staff who request the cooperation of the Data Protection Officer when they are verifying the Cedefop's compliance with Regulation (EU) 2018/1725 as regards personal data breaches. <u>Data categories:</u> For the purpose of this processing operation, in particular the following personal data are processed: • contact details of the controllers and delegates controllers of Cedefop involved in a personal data breach; • contact details of Cedefop staff who inform the Data Protection Officer of a personal data breach, and/or are involved in managing the personal data breach; • contact details of any other individual who informs the Data Protection Officer of a personal data breach; • contact details of the responsible staff of Cedefop's processor (if relevant) who inform the Data Protection Officer of a personal data breach, and/or are involved in managing the personal data breach; •contact details of the staff of the EDPS who request the cooperation of the Data Protection Officer when they are verifying the Cedefop's compliance with Regulation (EU) 2018/1725 as regards personal data breaches; • other contact details of staff who were involved in the incident; • personal information of the individuals who were affected by the breach. The provision of the above-mentioned personal data is necessary for the efficient monitoring by the Data Protection Officer and supervision of compliance by the EDPS.
9.	Time limit for keeping the data	The time-limits for storing personal data are as follows: The files containing personal data breaches are kept for 10 years, and then eliminated. Those records within these files that may include special categories

		of data will be eliminated prior the end of retention period established for 10 years, following the relevant records processing operation.
10.	Recipients of the data	Cedefop's staff responsible for carrying out this processing operation. 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. Data subject. Staff of the EDPS who request the cooperation of the Data Protection Officer when they are verifying the Cedefop's compliance with Regulation (EU) 2018/1725 as regards personal data breaches.
11.	Are there any transfers of personal data to third countries or international organisations? If so, to which ones and with which safeguards?	N/A
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. Access by Cedefop internal users for the internal part of documentation is password-protected.
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 publication on the Cedefop web portal.