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
	Electronic Signatures	
1.	Last update of this record	07/04/2021
2.	Reference number	CDFNOT092 – Electronic Signatures
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 / role: DRS Department for Resources and Support / Head of DRS Contact form for enquiries on processing of personal data to be preferably used: noc@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)	Cedefop
6.	Name and contact details of processor (where applicable)	• Cedefop is the owner and controller of electronic signature assets. • Cedefop takes charge of the management of the electronic signature service systems and data processing operations and uses the services of suppliers

		(HARICA, DigitalSign) who act as data processors, under specific contract with Cedefop. • **European Commission EU-Sign service** which provides the platform used by the Cedefop staff when they need to sign a document using the DigitalSign qualified digital signature. • The supplier's corporate details are: o **DigitalSign** – Certificadora Digital, S.A. (for Qualified Electronic signatures) Largo [e. Bernardino Ribeiro Fernandes, 264835-489 Nespereira – Guilmarães, Portugal. Certificate authority who handles the contract of the European Commission related to digital certificates o **HARICA** - GREEK ACADEMIC NETWORK (GUnet), University of Athens, Network Operation Center, Panepistimiopolis Ilissia, 15784 Athens, Greece
7.	Very short description and purpose of the processing	To process handling of electronic signatures, in order to validate and/or extend electronic signatures and/or seals on electronic documents, either qualified or advanced, depending on the qualification of the certificate presented by the end user and its support, according to the eIDAS regulation. The aim of electronic signing is to modernise business processes, lessen the administrative burden and reduce the use of paper in Cedefop, while pertaining to the established levels of assurance and legal effect. The processing under electronic signature service includes: • authentication and access rights • handling the personal information for issuing the qualified certificates (ID document information, mobile phone number) • handling of the electronic signatures • providing support to all the users of the service both for issuing the certificates and handling the signatures

		• information handling for service management purposes (including statistical reports, dashboards) Cedefop is using 2 discrete services: 1. an electronic signature service, namely EU Sign, which is limited to the staff of the European Commission and other EU Institutions, Agencies and Bodies according to which, personal data processing happens for the following 2 purposes: A) The processing for handling the electronic signatures, in order to create, validate and/or extend electronic signatures on electronic documents, either qualified or advanced, depending on the qualification of the certificate presented by the end user and its support, according to the eIDAS regulation. B) The processing for identification of natural users in order to allow the partners Qualified Trusted Service Provider QTSP to issue "remote" qualified certificates (stored in a Qualified Signature Control Device QSCD device of the QTSP). C) In the case of EU-Sign the information is stored on the EU-Sign platform maintained the Commission. 2. an eSeal service provided by HARICA, which is limited to Cedefop and its organizational units. In this case, personal data processing happens for handling the electronic signatures, in order to create, validate and/or extend electronic seals on documents, either qualified or advanced, depending on the qualification of the certificate presented by the end user and its support, according to the eIDAS regulation. D) In the case of Harica, the information is stored on the desktop and laptop of the user who issues the certificate and receives it onto his/her computer. The legal basis of the processing is Article 5 (a) of Regulation (EU) 2018/1725 in that it supports core tasks of Cedefop in Regulation (EU) 2019/128.

8.	Description of categories of persons whose data the EDPS processes and list of data categories	**Data subjects**: end users, such as Cedefop staff, Seconded National Experts, trainees and any other person who have been provided with a Cedefop email address (i.e. one with suffix cedefop.europa.eu) receive electronic certificates for signing and make use of them with the purpose of e-signing documents or records either as persons (e-signature) or on behalf of the organisation or unit (e-seal). External contractors will be provided an e-signature on a case-to-case basis, upon approval by the Head of DRS. **Categories of personal data processed**: 1. Under EU-Sign service: a) Personal data related to the user of the electronic signature service: • Name, Surname (as per Identification Authentication management service IAMS) • Commission generated User ID of the requestor (as per IAMS) • professional e-mail address (as per IAMS) • data present on the signing certificate for users of the remote signing functionality (defined by the issuer, it can be/but not limited to: first/last name, date of birth, ID Number, membership, title/role) b) Additionally, for the individuals that request a "remote" qualified certificate for electronic signature, EU-Sign will process the flowing information: • Given Name(s), Surname(s) as per the ID document • ID document type • ID document number • Country issuer of the ID document • issuance end expiration date of the ID document • copy of the ID document • nationality • mobile phone number • data related to the organization the user works for

		This information is then transferred to the Qualified Trust Service Provider (QTSP) who issues the qualified certificate for electronic signature. Once the certificate is correctly issued, the data is deleted from EU-Sign database. For the individuals receiving a "remote" qualified certificate for electronic signature, after the certificate is issued EU-Sign will process: • Commission generated User ID of the requestor (as per IAMS) • date of certificate request • date of the certificate issue • information about certificate validity • encrypted information related to the certificate (e.g. public key, certificate alias, etc.) c) Administrative data related to the user of the electronic signature service (from IAMS): • JobID (Administrative position) • Organization (DG/EUI/Agency/Body) d) Technical data related to the usage events of electronic signature service: • Type of operation (sign/seal, verify, extend) • date/time of the operation request • Target of the operation (which value/policy of the signature (e.g. EC-Internal, Qualified Electronic Signature) e) Log files: • Each time the user performs a signature, EU-Sign will store the above-mentioned categories with the exception of personal data related to signing certificates. Additionally, a history of all operations performed by an individual will be kept for troubleshooting purposes. 2. Under eSeal service (advanced or qualified): • Name • Title/Position • Email Address • Mobile number

9.	Time limit for keeping the data	The administrative time limits for keeping the personal data per data category are: Joint scope (EU-Sign, eSeal service): • Personal data related to the user of the services: 25 months EU-Sign scope: • Administrative data related to the user of the service: 25 months • Technical data related to the usage events of the service: 25 months • Log files: 6 months • History of all operations performed by an individual: 25 months • Personal data (as per the ID document) for individuals requesting "remote" certificates for the electronic signature: until the certificate is issued (2-5) days • Data related to the user who received a "remote" certificate: during the whole validity of the certificate plus 6 months • The object ((un)signed data carrier, signature file) to which the operation (sign, validate, extend) is applied: for the duration required to complete the request (sign, validate, extend) • Personal data transferred to the QTS: up to 20 years eSeal (HARICA) scope: • Personal data transferred to the Qualified Trusted Supplier QTS: up to 7 years, after the expiration/revocation of the eSeal certificate.
10.	Recipients of the data	The origin of the data recipients can be of the following types: • **within the EU organisation**: administrators of the electronic signature service; any Commission user of the electronic signature service has access to the personal information present in the signer certificate as per the signed documents. • **outside the EU organisation**: anyone in the world receiving a signed document has access to the personal information on the certificate on

		the signed document; the administrators of electronic signature service partner QTSPs for the data related to the requests for "remote" certificates for qualified electronic signature and for the data related to the eSeal service.
11.	Are there any transfers of personal data to third countries or international organisations? If so, to which ones and with which safeguards?	No data transfer to countries outside the EU, EEA or international organisations.
12.	General description of security measures where possible.	Regarding EU-Sign: All necessary measures are placed in accordance to Commission Decision (EU, Euratom_ 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission. EU-Sign takes all reasonable measures to protect the Confidentiality, Integrity and Availability of information stored in EU-Sign, whether provided by other IT systems or by the individual directly. The measures include the use of physically separate machines, located in computer rooms (EC DIGIT data centres) that are protected against unauthorized physical access. Regarding eSeal service: HARICA, the provider of the eSeal service, takes all reasonable measures to protect the Confidentiality, Integrity and Availability of information created and stored, whether provided by other IT systems or by the individual directly. The measures include the use of physically separate machines, located proprietary data centres that are protected against unauthorized physical access and is the organization is annually audited against ETSI EN & eIDAS criteria.
13.	For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	Available on intranet for all Cedefop staff. Also provided in privacy statements of specific Cedefop online conferences and events.