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
Microsoft 365 Documents, Records management and Collaboration		
1.	Last update of this record	19/10/2022
2.	Reference number	CDFNOT005 - Microsoft 365 Documents, Records management and Collaboration
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: Department for Resources and Support (DRS) / ICT
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. Cedefop disables operations for which Microsoft acts as controller, specifically, the optional “connected experiences”.
6.	Name and contact details of processor (where applicable)	- Cedefop ICT staff who provide, manage and support the M365 system - Microsoft Ireland (South County Business Park, One Microsoft Place, Carmanhall and Leopardstown, Dublin, D18 P521, Ireland), who provides the M365 platform.

		- Microsoft Ireland's subcontractors, namely Microsoft corporation (USA) and other individual subcontractors. A list of Microsoft's current sub processors is available at https://aka.ms/servicesapprovedsuppliers
7.	Very short description and purpose of the processing	To allow staff (or other persons working for Cedefop) to access and use communication and collaboration functionality in the context of performing Agency tasks, including: Communication and collaboration using Microsoft Teams; Collaboration on documents using Microsoft SharePoint Online; Use of integrated Office 365 functionality within these tools. Cedefop uses MS365 as an online platform offering document and record management as well as collaboration, in line with its "ICT & Digital Strategy 2021-2024". Almost all of Cedefop's files and collaboration content is stored on M365. A. **Cedefop ICT staff** is processing the data so as to ensure the good functioning of the service provided. More specifically, the purposes are: 1. ID and access management, i.e. create accounts, provide access or amend who has access where, in a central way, as needed and requested. 2. Technical assistance, support and troubleshooting, including Security incident management 3. Backups of data for security and availability purposes. 4. Assistance to data subjects in exercising their rights B. **Microsoft** is processing the data so as to provide to Cedefop the M365 online services. More specifically, the purposes are: 1. To provide the platform (delivering functional capabilities as licensed, configured and used), e.g. by storing the data there. 2. For Troubleshooting (preventing, detecting and repairing problems affecting the operation of the services). 3. For Ongoing improvement (installing the latest updates and capabilities, and making improvements to user productivity, reliability, efficacy and security).

		C. In addition to this, **Microsoft** has been granted permission to process a small subset of personal information (i.e. the "Service Generated Data" and some "Identification data") for their own, internal business functions in the context of providing the Office 365 service. These functions are the following (exhaustive list): 1. Billing and Account Management (identification data, service generated data); 2. Compensation (e.g. calculating employee commissions and partner incentives) (service generated data); 3. Internal Reporting and Business Modelling (service generated data); 4. Combatting fraud, Cybercrime, and Cyberattacks that may affect Microsoft or Microsoft Products (identification data, service generated data); 5. Improving Core Functionality of Accessibility, Privacy and Energy Efficiency (service generated data); 6. Financial Reporting and Compliance with Legal Obligations (subject to the limitations on disclosure of Processed Data) (identification data, service generated data)
8.	Description of categories of persons whose data Cedefop processes and list of data categories	**Data subjects**: Cedefop staff members (officials, temporary agents, contract agents) as well as Seconded National Experts, interim agents and trainees. Partially, also: external contractors, external stakeholders (such as network members, expert groups, management board members), participants in Teams meetings. **Categories of personal data processed:** 1. Identification data - Last name, first name, e-mail - Department, position, staff number - Business and personal landline phone and mobile

		2. Content data - All of Cedefop's files/documents, records, video recordings and other collaboration content (e.g. chat messages). Additionally, transient data such as video/audio calls. The authoritative listing of all specific personal data processed can be found in the individual Data protection records, as per the Annex 5 of Cedefop's M365 Data Protection Impact Assessment (DPIA)[1]. 3. Diagnostic / system (or service)-generated / connected-experiences data - Secondary (meta-)data (e.g. diagnostic information and logs files) that are generated through the use of the Microsoft Office applications and the M365 system, could also contain personal data (i.e. personal identifiable information). These include logs of actions such as "Access File", "Create folder", etc., including the pseudonymised username of the user who performed the action and the anonymised IP address. As there is a possibility that these are connected to a specific person, even if the use of other datasets would be needed for this, they are still considered as personal data under the EUDPR. - The above (meta-)data are retrieved, aggregated and pseudonymized to produce the "*Aggregated*" system-generated data. 4. Sensitive Non-Classified (SNC) data, as defined in DIR 07/2019 "Rules on the marking and handling of sensitive non-classified information at Cedefop" [2] will be protected by encryption and through the application of appropriate M365 "Sensitivity labels". **Special categories / Sensitive data:** Some of Cedefop's processing operations using M365 include the handling of sensitive data, including special categories of personal data within the meaning of Article 10 of the EUDPR[3].

		Cedefop operations that could possibly include sensitive personal data and are using M365 are for example the following operations/processes (non-exhaustive list): - CDFNOT037 Personal files - CDFNOT038 Traineeship grant - CDFNOT043 Appeals - CDFNOT045 Access control to premises - CDFNOT075 Requests for Teleworking - Case No 2008-196 Traineeship selection and traineeships - Case no 2009-122 Staff Recruitment - Case No 2010-0001 / 2008-194 Health Data and Medical Files - Case No 2011-540 Anti-harassment - 2007-582 – Administrative inquiries and disciplinary procedures at Cedefop Any personal data of special categories within the meaning of Article 10 of the EUDPR, will be mandatorily protected by the application of the corresponding sensitivity labels and the special technical measure of "Double-key encryption" (DKE).
9.	Time limit for keeping the data	- The retention periods of "*Identification*" and "*Content*" data are defined in the respective data protection records and follow Cedefop's records management retention schedule. - The "*Service-generated*" audit data are normally kept for up to 1 year. Should Cedefop so require, they could be kept for up to 10 years. - The "*Aggregated service-generated data*" are kept for up to 6 months.

[1] RB(2022)00117, Data Protection Impact Assessment (DPIA) for the Microsoft 365 (M365) platform at Cedefop, https://livelink.cedefop.europa.eu/livelink/livelink.exe?func=ll&objaction=overview&objid=29584102

[2] DIR 07/2019 "Rules on the marking and handling of sensitive non-classified information at Cedefop: https://livelink.cedefop.europa.eu/livelink/livelink.exe?func=ll&objaction=overview&objid=27965184

[3] personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs; trade-union membership; genetic data, biometric data processed solely to identify a human being; health-related data; data concerning a person's sex life or sexual orientation.

		- The "*Essential services*" diagnostic data that Microsoft is processing are kept for up to 1 year. - In case the subscription with Microsoft expires/terminates and Cedefop deletes all data there, they will still stay in Microsoft's servers for up to 180 days. During this period, all contractual obligations still remain valid.
10.	Recipients of the data	For the selected purposes, specific Cedefop personal data in M365, as detailed above, can be accessed by authorised Cedefop staff, Cedefop ICT external contractors and Microsoft staff, according to the "need-to-know" principle[4]. The specific recipients are: A. Cedefop staff, for the purposes listed under 7.A of the current document. Specifically: 1. Designated Cedefop ICT staff and specific ICT external contractors, subject to signed Non-disclosure and confidentiality agreements 2. Cedefop's Record manager and backup Record manager See section 4.2 of the DPIA for more details on the two above B. Microsoft staff, for the purposes listed under 7.B and 7.C of the current document. Specifically: 1. Microsoft engineers 2. Microsoft sub-processors (the agreement with Microsoft lists all Microsoft sub-processors– see section 12.5 of the DPIA for more discussion on this. A list of Microsoft's current sub processors is available at https://aka.ms/servicesapprovedsuppliers C. Access to the personal data may be granted also to authorized staff in public authorities or audit control or investigation bodies such as: Court of Auditors, Internal Audit Service of the European Commission, European Anti-Fraud Office (OLAF, European Ombudsman, the European Data Protection Supervisor, the General Court or the European Court of Justice.

[4] other M365 users could also receive content data when shared with them (on a need-to know basis and with relevant permissions)

11.	Are there any transfers of personal data to third countries or international organisations? If so, to which ones and with which safeguards?	In most cases, no personal data is transferred outside the EU/EEA. All customer data at rest, including all back-up data are stored within the geolocation of the tenant and for Cedefop that is the EU/EEA territory. However, for certain limited categories of personal data, Microsoft Ireland may transfer personal data to the USA or any other country in which Microsoft or its sub-processors operate. - The "Diagnostic/telemetry" ("Essential services" as per section 3.3.1 of the DPIA) data collected by Microsoft are located in the US. - The "Aggregated service-generated" data (as per section 3.3.3 of the DPIA) are transferred to the US for processing and storage. - The "Connected experience" data (as per section 3.3.4 of the DPIA) are processed (but not stored) by Microsoft on US-based servers. Safeguards applied for the transfers: - Microsoft Ireland has signed with Microsoft Corp. the Standard Contractual Clauses ("SCCs") (module three: processor to processor)[5] which cover all transfer scenarios and constitute the legal tool on which the transfer is based. The new SCCs are part of the ILA contract and have been updated with an Additional Safeguards Addendum[6]. - A specific Transfer Impact Assessment was performed as part of Cedefop's M365 DPIA. Based on this, supplementary measures are taken (mainly the use of encryption), with which the transfer of the personal data concerned to the United States is effectively subject to appropriate safeguards - Further technical measures applied are: Pseudonymisation, Aggregation
12.	General description of security measures where possible.	Specific technical security measures taken are (note: references are to the DPIA): - Application of full encryption at-rest and in-transit (see section 7.4.1)

[5] The Commission adopted on the 4th of June 2021 the Implementing decision (EU) 2021/914 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679. According to recital 8 of the latter decision, these standard contractual clauses may be used by processors, which process personal data on behalf of an EUI and transfer personal data to a sub-processor located in a third country.

[6] DIGIT ILA (version 2021), page 38, Data Transfers; Attachment 2 Standard Contractual Clauses (processors).

		- Pseudonymisation and aggregation of Service-generated and Diagnostic logs (see sections 5.3, 5.4, 7.1) - Application of document-level encryption for the protection of Sensitive Non-Classified (SNC) information, through the use of M365 "Sensitivity labels" (see section 12.7) - Double-key encryption (DKE) for Special categories of personal data (see section 3.4) - Activation of detailed inviolable Audit logs and corresponding alerts (see section 12.7) - Disabling diagnostic logs collected by Microsoft of type "Required" and "Optional" (Option "No diagnostic data is collected and sent to Microsoft"). See Section 5.3. - Disabling of Microsoft service "optional connected experiences (termed "Controller Connected Experiences"), for example Bing smart lookup, LinkedIn Resume Assistant (see section 5.5) - Disabling of Microsoft features of "Standalone Online services". These include for example products such as Bing maps, Cortana, Github enterprise (see section 5.5)
13.	For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	*Privacy statement available on Cedefop's Intranet:* Privacy notice - Microsoft 365 document management *Invitations to register for participation in specific events also contain link to corresponding event privacy notice*