

Cedefop record of processing activity

Microsoft InTune

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 InTune		
1.	Last update of this record	02/09/2024
2.	Reference number	CDFNOT115
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 Thessaloniki, GREECE Telephone: (+30) 2310-490111 Email: info@cedefop.europa.eu Responsible department or role: Department for Resources (DRS)/ ICT service Contact form for enquiries on processing of personal data to be preferably used: ict-service@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)	• “Bluestream” is the external contractor of Cedefop (under 2022-FWC2_AO_DRS_SAN-SAK_ICTSS III_001_22 Lot 1, “<i>ICT Services related to Microsoft-related Server and Server Applications</i>”). Its contractors provide technical support and consultancy relating to Microsoft-based servers and desktop/laptop PCs. BLUESTREAM SOLUTIONS LTD, 10th Km Thessalonikis-Thermis, 57001 Thessaloniki Greece. Legal representative: Georgios Vasdekis, vg@bluestream.gr • Microsoft Ireland Operations Ltd., as the processor for Sharepoint (the tool for processing and storing information and documents by Cedefop). Contact details: South Country Business Park, One Microsoft Place, Leopardstown, Dublin 18, D18 P521, Ireland, Tel. +353 1 706 3117.
7.	Very short description and purpose of the processing	Purpose of the processing: The Microsoft InTune is a cloud-based device management software, running online at EU-based servers of Microsoft. It connects to all of Cedefop’s Windows servers, laptop/desktop PCs and potentially mobile phones to provide complete management: installation of software/apps, application of global group policies to configure in detail the applications in terms of functionality as well as security policies, review of system performance. The service is described at: https://learn.microsoft.com/en-us/mem/intune/
8.	Description of categories of persons whose data Cedefop processes and list of data categories	The categories of persons whose personal data are processed are Cedefop staff members, Seconded National Experts, trainees, interim agents, staff of external contractors. Categories of personal data: • Personal information: first name, last name, e-mail, username • Device Information: ○ Device Name: The name of the device, often containing user-identifiable information. Example: JDoe-Laptop, W10-9995

		○ Device ID: A unique identifier for the device, which may be tied to the user. Example: IMEI: 356789123456789 ○ Operating System: Information about the OS on the device, which can sometimes indicate user behavior or preferences. Example: Windows 10 Pro ○ IP Address: The IP address used by the device, which can be tied to a location or user. Example: 192.168.1.100 ○ MAC Address: A unique identifier for the device's network interface. Example: 00-14-22-01-23-45 ○ Device Manufacturer and Model: Brand and model of the device ○ Example: Lenovo Laptop F345 ● Application Data ○ Installed Applications: A list of applications on the device, which could reveal user preferences or habits. Example: Microsoft Word, Zoom, Firefox ○ Application Usage: Data on how often and when certain applications are used, which can provide insight into user behavior. Example: Zoom used for 3 hours on 09/01/2024 ● Location Data ○ Device Location: Geographic location data associated with the device, if location tracking is enabled. Example: Latitude: 37.7749, Longitude: -122.4194 (San Francisco, CA) ● Usage and Activity Logs ○ Login/Logout Times: Records of when users log in and out, providing insight into their work patterns. Example: Login at 08:00 AM on 09/01/2024 ○ Device Activity: Data on how and when the device is used, potentially revealing user behavior.
--	--	---

		Example: Device unlocked at 09:00 AM - Security Incident Data - Threat Detection: Information on any security threats detected on the device, possibly linked to user actions. Example: Malware detected on JDoe-Laptop on 09/02/2024 - Security Incidents: Records of security incidents, such as unauthorized access attempts, which may involve user data. Example: Failed login attempt by user jdoe at 10:00 AM on 09/01/2024 For a full list see: https://learn.microsoft.com/en-us/mem/intune/protect/privacy-data-collect
9.	Time limit for keeping the data	As long as the device is enrolled in InTune, and is therefore an active part of Cedefop's network, a basic set of data (e.g. device name, username, etc.) is kept for this period. The audit, usage and activity logs are removed after 1 year.
10.	Recipients of the data	- Cedefop ICT administrator staff - Staff of external contractors (Bluestream)
11.	Are there any transfers of personal data to third countries or international organisations? If so, to which ones and with which safeguards?	No. As per Microsoft's EU Data Boundary commitment, all data of InTune are kept within EU boundary.
12.	General description of security measures where possible.	Cedefop implements extensive technical and organisational measures for safeguarding security, as documented in its ICT Use and Security Policy. Administrator access to InTune data is restricted to very few experts and external consultants, whose accounts are protected with Two-factor Authentication. Intune processes personal data with ISO certified systems. For more information, see the Service Trust Portal.

		Microsoft uses strict controls to govern access to data, granting the lowest level of access required to complete key tasks and revoking access when it's no longer needed. We secure and control access to data by using role-based administration control (RBAC), as per RBAC with Microsoft Intune .
13.	For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	