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
		Atlassian cloud software (Trello, Jira, Confluence, Access)
1.	Last update of this record	15/03/2023
2.	Reference number	CDFNOT006 - Atlassian cloud software (Trello, Jira, Confluence, Access)
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)	Cedefop is controller of processing of personal data (and Atlassian is a processor on behalf of Cedefop) in connection with the Atlassian Jira Work Management, Jira Service Management, Confluence, Access and Trello services. However, Atlassian is a controller of personal data for own legitimate business purposes in connection with the operation, support and/or use of the services (e.g. Atlassian cloud account profile). Cedefop signed and filed a Data Protection Addendum with Atlassian.

6.	Name and contact details of processor (where applicable)	• Designated Cedefop ICT staff and contractors responsible for helpdesk or other ICT-related tasks • Atlassian US, Inc.; Atlassian PTY Ltd, Trello Inc. who provide the Jira cloud, Jira Work Management, Jira Service Management, Confluence, Access and Trello platforms. • Atlassian Sydney (Global HQ), Level 6, 341 George Street, Sydney, NSW 2000, Australia. • Atlassian sub-processors: https://www.atlassian.com/legal/sub-processors
7.	Very short description and purpose of the processing	To allow staff (and/or other persons working for Cedefop) to access (Access) and use project management (Jira Work Management, Trello), helpdesk (Jira Service Management) and content collaboration (Confluence) functionality in the context of performing Agency tasks (e.g. helpdesk support tickets, ICT-related documentation, project management, task tracking etc.). Cedefop uses Atlassian cloud solutions in line with the Cloud First principle in its "ICT & Digital Strategy 2021-2024". • Trello: visual project management using Kanban boards; • Jira Work Management: for teams to manage projects and processes (e.g. collaborate, align, and deliver work) across the agency; • Jira Service Management: helpdesk and service management; • Confluence : content collaboration (e.g. wiki, documents, discussions) ; • Access: identity and access management for data security & governance (connects Cedefop's Atlassian cloud products to Cedefop's identity provider). A. **Cedefop ICT staff** is processing personal data to ensure the good functioning of the services 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. **Atlassian** processes personal data for Atlassian's legitimate business purposes such as: 1. To facilitate security, fraud prevention, performance monitoring, business continuity and disaster recovery in order to protect Customers, End Users and Atlassian; 2. To engage and to provide support and assistance to Cedefop and End Users as requested from time to time; 3. To comply with legal and financial reporting obligations; 4. To administer the Services, including to calculate usage-based billing; 5. To derive insights in order to maintain, develop, and improve the Services and support, including for research and development purposes; 6. To derive insights in order to inform internal business analysis and product strategy.
8.	Description of categories of persons whose data Cedefop processes and list of data categories	**Data subjects**: • Designated Cedefop ICT staff and contractors responsible for helpdesk or other ICT-related tasks; • Designated staff in DCM and DVQ departments (and their contractors) for project-related support tickets; • Cedefop staff (officials, temporary agents, contract agents as well as Seconded National Experts, interim agents and trainees) in that they are users and can create helpdesk tickets. **Categories of personal data processed** Cedefop as a controller processes the following categories of personal data: User Account Information (Jira / Confluence cloud, Jira Work Management, Jira Service Management, Trello), for example: • Atlassian identifier associated with user account;

		• About Me; • Avatar Image and URL; • Full name; • Email address; • Time zone. Personal Identification (Jira Work Management, Jira Service Management, Trello), for example: • IP address; • Cookie information (Trello); • Language setting; • Location/ Region/ City; • Phone numbers; • Screen name/ Handle/ Nickname. Employment Information (Jira / Confluence cloud, Jira Work Management, Jira Service Management, Trello), for example: • Job title / role; • Office / location; • Company/organization. Personal data included in Cedefop's generated content, for example: • Information and any personal data contained in the Jira Work Management and Jira Service Management support tickets created by Cedefop users (e.g. support ticket title,description, attachments and metadata); • Information and any personal data contained in the Trello boards, lists and cards created by Cedefop users. **Atlassian as a controller processes personal data relating to or obtained in connection with the operation, support or use of the Services, e.g.:**

		• User Account Information: e.g. pseudonymous Atlassian IDs, Cloud IDs, Site IDs,Tenant ID, Segment Anonymous IDs; • Payment and billing information, to the extent it includes personal data; • Device and connection information, for example: IP address, cookie information, device information, browser information; • Information on the use of the Services, for example: event name (i.e., what action the user performed); event timestamp; page URL, referring URL; • Support data: personal data provided through various Atlassian support channels, including for example Atlassian ID, SEN (Support Entitlement Number), username, contact information and any personal data contained within a summary of the problem experienced or information needed to resolve the support case; • Also user-generated content (If any is submitted as attachments via support tickets). **Special categories / Sensitive data:** Cedefop's use of Atlassian cloud products does not process sensitive / special categories of personal data within the meaning of Article 10 of the EUDPR[1].
9.	Time limit for keeping the data	**Jira / Confluence cloud, Jira Work Management, Jira Service Management:** Upon termination, Customer accounts are deactivated within 15 days (for monthly subscriptions) and 17 days (for annual subscriptions) after the end of the Customer's current subscription period. Atlassian retains data for deactivated products for 15 days (for evaluation licenses) or 60 days (for Free, Standard, and Premium product plans) after the end of the Customer's current subscription period. Upon deletion, an archive of the data is kept for an additional 30 days.

---

[1] 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.

| | | Jira tickets, attachments and associated metadata are kept in the Atlassian cloud platform as a repository and Cedefop records classification and retention policies apply.

Trello:
On termination of a Trello enterprise contract, and at the request of the Customer, the data belonging to the enterprise teams will be completely removed from the live production database and all file attachments uploaded directly to Trello will be removed within 30 days. The team's data will remain in encrypted Trello database backups until those backups fall out of the 90-day backup retention window and are destroyed in accordance with Trello's data retention policy.

Cedefop keeps Trello data in the Trello platform as long as it is needed for collaboration. No data is kept in the records bank. |
|---|---|---|
| 10. | Recipients of the data | A. Designated Cedefop staff and specific external contractors who use the platform;
B. Cedefop's Records manager and backup Records manager;
C. Atlassian staff (subject to duty of confidentiality)
D. Atlassian sub-processors (subject to duty of confidentiality and written agreements with same obligations as Atlassian)
E. 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. |
| 11. | Are there any transfers of personal data to third countries or international organisations? If so, to which ones and with which safeguards? | Atlassian is a global company with global headquarters in Sydney Australia and US headquarters in San Francisco, CA. Atlassian may transfer customer personal data wherever they (or their third-party service providers) operate for the purpose of providing services: |

		• Atlassian cloud account profile (Identity): stored in United States; and may be processed in Australia, Germany, India, Netherlands, United States; • Jira and Confluence Cloud, Jira Work Management, Jira Service Management and Trello: stored in Asia-Pacific, Europe (EEA), United States, may be processed in Australia, Brazil, Germany, India, Japan, Malaysia, Mexico, Netherlands, New Zealand, Philippines, Poland, Turkey, United Kingdom, United States *Safeguards applied for the transfers:* • Transfer tool: Cedefop signed and filed with Atlassian a Data Processing Addendum (DPA) which identifies EC Standard Contractual Clauses (SCCs) as the Transfer Mechanism. The DPA includes "Module 1 (controller to controller transfer terms) to address transfers of the limited personal data Atlassian processes as a controller, Module 2 (controller to processor transfer terms) and Module 3 (processor to processor transfer terms) of the SCCs; • Atlassian's Transfer Impact Assessment was reviewed by Cedefop; • Other supplementary measures: data is encrypted both in transit and at rest, in-scope product content at rest pinned to a EU location.
12.	General description of security measures where possible.	Specific technical security measures taken include (see also DPA Exhibit B: Technical and Organizational Security Measures): • Any customer data in Atlassian cloud products is encrypted in transit over public networks using TLS 1.2+ with Perfect Forward Secrecy (PFS) to protect it from unauthorized disclosure or modification; • Data drives on servers holding customer data and attachments in Jira Software Cloud, Jira Service Management Cloud, Jira Work Management, Confluence Cloud, and Trello use full disk, industry-standard AES-256 encryption at rest; • Atlassian maintains a formal security management program which includes: written information security policy and framework, periodic risk assessments, prompt review of security incidents, and formal audit standards (AICPA SOC 2 Type II report, ISO27001, and NIST 800-530);

		• Employee screening, training, access and controls; • Compliance program which includes independent third-party audits and certifications; • Vulnerability management processes; • Cedefop administrators to configure and enforce password complexity requirements for Cedefop domain users via Atlassian Access: https://support.atlassian.com/security-and-access-policies/docs/manage-your-password-policy/; • 2 factor authentication • Tenant separation; • Data retention and destruction standard; • Secure deletion.
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 web portal and records management system.*