

ANNEX K3

Privacy Level Agreement (PLA)

1.1 Objective

The Privacy Level Agreement (PLA) provides a systematic way to communicate the level of personal data protection offered by the cloud service provider (CSP) to Cedefop. The PLA is based on Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing ('A.29WP05/2012') and is used to anchor PLA to the required legal provisions of the applicable EU data protection foundation.

As Cedefop intends to process personal data to the cloud the following parameters need to be considered:

- The definition of its security, privacy and compliance requirements
- The identification of the data/processes/services that are moved to the cloud
- The analysis and assessment of the risks involved
- The definition, responsibilities and tasks for the security controls implementation
- The determination of the obligations that must be monitored regarding the activities of the service providers

Cedefop mandates that its ICT Security requirements by the CSP are the following:

Cedefop mandates that the CSP is compliant with the Data Protection Regulation (45/2001) and Directive 95/46 as regards to all the processes that will take to host and support the cloud application.

The Skills panorama project provides a registration page where the users are requested to register to the site, thus providing personal data about themselves.

Cedefop recognises that although the hosting of this project on the cloud (by a CSP) has many advantages, it also includes risks which must be addressed. The tables below require from the CSP to provide information on how they comply with the current data protection regulation while providing cloud services for Cedefop.

1.2 MANDATORY REQUIREMENTS TO BE FULFILLED

TABLE 1

	IDENTITY OF THE CSP (AND OF REPRESENTATIVE IN THE EU AS APPLICABLE), ITS ROLE, AND THE CONTACT INFORMATION FOR THE DATA PROTECTION INQUIRIES	EU based	Non-EU based
	Specify:		
1.	CSP name, address, and place of establishment;		
2.	Its local legal representative(s) ;		
3.	Its data protection role in the relevant processing (i.e., processor or sub-processor)		
4.	Contact details which the customer can use to submit personal data protection related inquiries.		
5.	Contact details of the Data Protection Officer or, if there is no DPO, the contact details of the individual in charge of privacy matters to whom the customer may address requests.		
6.	Contact details of the Information Security Officer, if there is no ISO/IEC (27001:2013), the contact details of the individual in charge of security matters to whom the customer may address requests.		
	WAYS IN WHICH THE DATA WILL BE PROCESSED		
7.	Provide details on the extent and modalities in which the Cedefop-data controller can issue its instructions to the CSP-data processor.		

TABLE 2

8.	Specify how the cloud customer will be informed about relevant changes concerning the relevant cloud service(s) such as the implementation of additional functions.	
9.	Specify the way that the right of access to and the right to rectify the data concerning the data subject is provided by this CSP.	
10.	How does the CSP guarantee fair processing in respect of the data subject (Art. 10 Directive 95/46/EC)? How does the CSP distinguish activities that are conducted to provide the agreed cloud service(s) (e.g., storage of data), activities that are conducted at the customer's request (e.g., report preparation or production) and those that are conducted at the CSP's initiative (e.g., back-up, disaster recovery, fraud monitoring)? What type of reports does the CSP provide to Cedefop to prove that the above measures are in place? How frequently does the CSP provide such reports to Cedefop?	

AO/DSL/AZU-JBU/SkillsPanoramaUX/004/16

	PERSONAL DATA LOCATION	
11.	Specify the location(s) of all data centres where personal data may be processed, and in particular, where and how they may be stored, mirrored, backed-up, and recovered.	
	SUBCONTRACTORS	
12.	Identify the subcontractors and sub- processors that participate in the data processing, the chain of accountability and approach used to ensure that data protection requirements are fulfilled.	
13.	Identify the procedures used to inform the cloud customer of any intended changes concerning the addition or replacement of subcontractors or sub-processors with the cloud customers retaining at all times the possibility to object to such changes or to terminate the contract.	
	DATA TRANSFERS	
14.	Indicate whether data is to be transferred, backed-up and/or recovered across borders, in the regular course of operations or in an emergency. If such transfer is restricted under applicable laws, identify the legal ground for the transfer (including onward transfers	

AO/DSL/AZU-JBU/SkillsPanoramaUX/004/16

	through several layers of subcontractors): e.g., European Commission adequacy decision, model contracts, Safe Harbour, Binding Corporate Rules (BCR). The tenderer should provide proof of any of the above, (the decision or model contract, or Safe Harbour registration, or Binding Corporate Rules) to Cedefop.	
	DATA SECURITY MEASURES	
15.	Specify the technical, physical and organizational measures in place to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized use, unauthorized modification, disclosure or access and against all other unlawful forms of processing.	
16.	Describe the concrete technical, physical, and organizational measures to ensure:	
	Availability: describe the processes and measures in place to manage the risk of disruption and prevent, detect and react to incidents, such as backup Internet network links, redundant storage and effective data backup and restore mechanisms;	
	Integrity: describe how the CSP ensures integrity (e.g., detecting alterations to personal data by cryptographic mechanisms such as message authentication codes or signatures);	

AO/DSL/AZU-JBU/SkillsPanoramaUX/004/16

Confidentiality: describe how the CSP ensures confidentiality from a technical point of view (e.g., encryption of personal data 'in transit' and 'at rest' authorization mechanism and strong authentication), and from a contractual point of view, such as confidentiality agreements or confidentiality clauses, and company policies and procedures binding upon the CSP and any of its employees (full time, part time, contract employees), and subcontractors (if any), who may be able to access the data and assurance that only authorized persons can have access to data;	
Transparency: describe which technical, physical and organizational measures the CSP has in place to support transparency and to allow review by Cedefop;	
Isolation (purpose limitation): describe how the CSP provides isolation (e.g., adequate governance of the rights and roles for accessing personal data (reviewed on a regular basis), access management based on least privilege principle, hardening of hypervisors (this is also relevant for the 'Integrity' section) and proper management of shared resources wherever virtual machines are used to share physical resources between different cloud customers);	
Describe how the CSP enables data subjects' rights of access, rectification, erasure, blocking and objection; in order to demonstrate the absence of technical and organizational obstacles to these requirements, including cases when data are further processed by	

	subcontractors	
	MONITORING	
17.	Indicate the options that Cedefop has to monitor and/or audit in order to ensure that appropriate privacy and security measures described in the PLA are met on an on-going basis. If such monitoring is possible, detail how (e.g., logging, reporting, [first- and/or third-party] auditing of relevant processing operations that are performed by the CSP or the subcontractors).	
	PERSONAL DATA BREACH NOTIFICATION "Personal data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a service provided by a CSP.	
18.	Specify how Cedefop will be informed of personal data and data security breaches affecting Cedefop's data processed by the CSP and/or its subcontractors, within what timeframe and how.	
19.	Specify how the competent Supervisory Authority(ies) and data subjects will be informed of personal data security breaches, within what timeframe and how.	
	DATA PORTABILITY, MIGRATION, AND TRANSFER BACK ASSISTANCE	

AO/DSL/AZU-JBU/SkillsPanoramaUX/004/16

20.	Specify the formats, the preservation of logical relations, and any costs associated to portability of data, applications and services.	
21.	Describe whether, how, and at what cost the CSP will assist Cedefop in the possible migration of the data to another provider or back to an in-house IT environment.	
DATA RETENTION, RESTITUTION AND DELETION		
22.	Describe the CSP's data retention policies and the conditions for returning the personal data and destroying the data once the service is terminated.	
	Data retention policy.	
23.	Indicate for how long the personal data will or may be retained.	
	Data retention for compliance with legal requirements.	
24.	Indicate whether and how Cedefop can request the CSP to comply with specific sectoral laws and regulations.	
	Data restitution and/or deletion.	
25.	Indicate the procedure for returning the personal data in a format allowing data portability, the methods available or used to delete data, and whether data may be retained after Cedefop has deleted (or requested deletion of) the data, or after the termination of the contract, and in each case the period during which the CSP will retain the data.	
ACCOUNTABILITY		

AO/DSL/AZU-JBU/SkillsPanoramaUX/004/16

26.	Describe what policies/procedures the CSP has in place to ensure and demonstrate compliance by the CSP and its subcontractors or business associates, including by way of adoption of internal policies and mechanisms for ensuring such compliance. CSPs need to identify the elements that can be produced and provided as evidence to demonstrate norms' compliance and behaviour. Evidence elements can take different forms, such as attestations, certifications, seals, third-party audits attestations, logs, audit trails, system maintenance records, or more general system reports and documentary evidence of all processing operations under its responsibility. These elements need to be provided at the (i) Organizational policies level to demonstrate that policies are correct and appropriate; at (ii) IT Controls level, to demonstrate that appropriate controls have been deployed; at (iii) Operations level, to demonstrate that systems are behaving (or not) as planned. Examples of evidence elements pertaining to the different levels are privacy seals (i), Certifications like CSA Certification - OCF Level 2 (ii) and logs (iii) produced by reliable monitoring and comprehensive logging mechanism, (iv) audit trails.	
	COOPERATION	
27.	Specify how the CSP will cooperate with Cedefop in order to ensure compliance with applicable data protection provisions: e.g., to enable Cedefop to effectively guarantee the exercise of data subjects' rights	

AO/DSL/AZU-JBU/SkillsPanoramaUX/004/16

	(right of access, correction, erasure, blocking, opposition), to manage incidents including forensic analysis in case of security breach).	
28.	Describe how the CSP will make the information necessary to demonstrate compliance available to Cedefop and supervisory authorities.	
LEGALLY REQUIRED DISCLOSURE		
29.	Describe the process in place to manage and respond to requests for disclosure of personal data by Law Enforcement Authorities; with special attention to notification procedures to interested customers, unless otherwise prohibited, such as a prohibition under criminal law to preserve confidentiality of a law enforcement investigation.	