

FINANCE AND PROCUREMENT

ANNEX K1

Hosting, regular administration and maintenance, monitoring and availability of the system

1. SCOPE

This annex describes the required services related to website hosting, administration and monitoring which aim at ensuring maximum system availability and stability.

These services shall be provided on a **fixed monthly price** basis.

1.1. General conditions for the provision of services

The tenderer must comply with the minimum service requirements presented here; however, the tenderer is allowed to propose an improved service level in each of the categories hereafter, as part of his offer for award criterion 2. If the tenderer proposes an improved service level, he will be bound to his proposal after acceptance by Cedefop and may not afterwards revert to the minimum requirements as set out in the present document.

The financial offer of the contractor shall reflect the technical offer of the tenderer and will be binding.

1.2. Fixed monthly price

The services described in this annex shall be provided on a **fixed monthly price** basis, **except when otherwise clearly specified by Cedefop**.

The fixed monthly price shall include hosting, regular administration and maintenance services, troubleshooting, security and improvement patches, delivery of monitoring reports, any software license annual fees, availability and support.

2. HOSTING AND REGULAR ADMINISTRATION SERVICES

2.1. General conditions

2.1.1. The hosting services that the contractor will be asked to provide under the contract will include:

Annex K1

- managed hosting on dedicated servers in a controlled environment with support, including operating systems and databases. Servers should be located in the EU.
- maintenance, administration and support of the operating system, applications and databases (including but not limited to upgrading, updating and patch management).

2.1.2. The contractor should provide the necessary hardware/software and services to match the web site and CMS needs.

2.1.3. The contractor shall provide a production environment and a staging environment for Cedefop use. Additionally the contractor will have its own testing/development environment.

2.1.4. During the contract life, the software for the different technologies and operating systems should not be older than two versions of the latest version in the market unless agreed otherwise with Cedefop.

2.2. Physical environment

2.2.1. All systems are to be housed in a secure and redundant environment physically located within a Member State of the European Union.

2.2.2. The contractor should provide a Data Centre that is either certified to be ISO 27001 (or equivalent) compliant or that conforms to those standards.

2.2.3. In the case that the Data Centre is not certified, then the contractor should provide evidence of conformance to those standards.

2.2.4. The contractor shall ensure that the hosting platform is backed-up to a remote location.

2.2.5. The Contractor shall have established procedures for Business Continuity Plan.

2.2.6. The contractor shall have established processes and procedures to ensure the security of the physical hosting environment, covering at least the following:

- Power supply;
- Environmental conditions;
- Security and Access Control;
- Fire / Flood suppression.

2.3. Capacity Management

Annex K1

- 2.3.1. Cedefop requires that the contractor have sufficient hosting capacity to meet the required performance as defined in the service level requirements.
- 2.3.2. The contractor shall ensure that the capacity at each layer of the platform is proactively monitored and managed .
- 2.3.3. The contractor shall ensure that prompt and adequate actions are taken before thresholds are reached .

2.4. Connectivity

- 2.4.1. The contractor shall provide multiple connections between their Data Centre and the Internet in particular ensuring fail-over if the connection fails. The Data Centre should have adequate bandwidth in order to meet the needs of Cedefop hosted systems .
- 2.4.2. The contractor shall provide a 100Mbps unmetered (i.e. without charging the amount of data passed) connection with the Internet as a minimum . This will be re-evaluated every year in respect of Cedefop needs.

2.5. Security

- 2.5.1. The contractor shall ensure the security of the Cedefop systems.
- 2.5.2. The contractor shall have documented security policies and procedures to ensure the physical and technical security of the Data Centre facilities; this should include firewall(s), vulnerability management, intrusion detection and denial of service attacks (both DOS and DDOS). The contractor should provide escalation procedures for security related issues and any security screening process for employees.
- 2.5.3. The contractor shall ensure that only authors authorised by Cedefop can put content on the web site. Secure access to CMS shall be possible from various locations. The CMS's editors shall be able to connect remotely to the CMS from any location with appropriate authorisation and in a secure way.
- 2.5.4. The contractor shall ensure that all webserver have Extended Validation SSL certificates.
- 2.5.5. The contractor shall apply, throughout the duration of the contract, policies and procedures to ensure that Cedefop systems are sufficiently protected against unauthorised access and system attacks. Along with continual security testing throughout the development process, the webserver must be regularly checked to ensure it is patched with latest software security releases .
- 2.5.6. Back-up and recovery requirements: back-up systems must ensure that in case of major incident (e.g. building fire with physical destruction of the servers) the service is fully reset in less than 12 hours. Images of the web

Annex K1

server must be taken daily to ensure the server can be rebuilt and fully restored if a major failure was to be identified.

- Daily backups for the last 8 days are required.
- Full weekly backups for the last 35 days are required.
- Full monthly backups for the last 6 months are required.

Requests to restore data should be satisfied within a maximum of one working day.

2.6. Availability and Service Level Key Performance Indicators (KPI)

2.6.1. Cedefop requires that all components comprising the Cedefop systems be available 24/7/365, except for scheduled maintenance. The contractor should take the necessary measures to address any incidents and restore the service.

2.6.2. Scheduled down time for the web services (front end) shall be between Friday 23:59 and Sunday 23:59 (Greek time).

2.6.3. Scheduled down time for the content management system (back end) shall be preferably between Friday 23:59 and Sunday 23:59 (Greek time). Downtimes of one hour are however acceptable during normal working hours if forecasted in advance.

2.6.4. The contractor shall liaise with Cedefop for the planning of scheduled downtime. Scheduled downtime should not exceed 4 occasions a year for a maximum of 12 hours.

2.6.5. Overall, systems downtime shall not exceed a total of 60 hours in one year.

Performance – response time:

2.6.6. On the website (front end), the average response time shall be less than 1 second with a maximum of 5% of the requests exceeding 2 seconds.

2.6.7. On the CMS (back end), an average of 2 seconds is acceptable, unless there is a special request, in which case it should show some sort of indication (e.g. hour glass cursor).

2.6.8. Additional Key Performance Indicators KPIs should be proposed by the tenderer:

- Maximum time a basic page takes to load in the Skills Panorama website
- Maximum time a dashboard takes to load in the Skills Panorama website
- Maximum time it takes to receive a document after requesting for it to be edited in the CMS editor
- Maximum time it takes to respond to any request/question from Cedefop with an acknowledgment message containing an indication of when the request/question will be answered

Annex K1

- Maximum time it takes to see in the Skills Panorama online urgent changes needed on pages not available through the CMS
- Maximum time it takes to receive proposals for or final content graphics (e.g. banners, sliders etc.) or marketing services or support materials (e.g. landing pages)
- Maximum time before an incident with severe or high impact or priority, affecting the users of Skills Panorama web resources, is resolved

The tenderer should also propose a reporting mechanism, tool, or for all Service level KPIs. Note that this needs to be part of the technical proposal.

2.7. Special clauses for the cloud provider

- 2.7.1. Cedefop data is protected by the Protocol of Privileges & Immunities applicable to the EU Institutions which means that they are inviolable. They shall be exempt from search, requisition, confiscation or expropriation. The property and assets of the Union shall not be the subject of any administrative or legal measure of constraint without the authorisation of the Court of Justice.
- 2.7.2. Therefore Cedefop data must be separated/partitioned and inaccessible from other service provider clients.
- 2.7.3. Cedefop data treated by the service provider (and all its (sub-) subcontractors) remain the exclusive property of Cedefop and may in no way be transferred to any other instance or person including national judicial authorities without the prior agreement of Cedefop's AIPN or delegated person.
- 2.7.4. Cedefop data may only be stored and treated on the territory of the European Economic Area (EEA = 28 EU countries + Island, Liechtenstein, Norway) + Switzerland.
- 2.7.5. The service provider must provide the list of all locations Cedefop data can be stored and or treated. The list must be accepted by Cedefop. Every additional data storage and or treatment location must be communicated in advance to Cedefop that can refuse the location or terminate the contract.
- 2.7.6. The service provider must provide the list of all subcontractors and eventually any sub-subcontractors that will store and or treated Cedefop data. The list must be accepted by the Cedefop. Every additional or replacement of (sub-)subcontractor must be communicated in advance to Cedefop that can refuse the subcontractor or terminate the contract.
- 2.7.7. The service provider and all its (sub-) subcontractors should not be subject to the Patriot Act (pending Court case Microsoft vs USA).
- 2.7.8. The contractor should implement appropriate technical and organisational measures to ensure a level of security appropriate to the

Annex K1

risks represented by the processing and the nature of the personal data to be protected.

- 2.7.9. Such measures shall be taken in particular to prevent any unauthorised disclosure or access, accidental or unlawful destruction or accidental loss, or alteration, and to prevent all other unlawful forms of processing.
- 2.7.10. For this reason the service provider needs to put in place the necessary technical and organisational measures to assure the data controller (Cedefop) that he (and all his sub-contractors) protect Cedefop's data against destruction, loss, modification, publication, without authorisation, during the treatment and its transmission over a network but also against any other illicit treatment.
- 2.7.11. The service provider needs to prove to Cedefop that he has an Information Security Management in place based on ISO27001, BSI or any other equivalent standard as CobiT and by preference certified for the services offered to the Cedefop.
- 2.7.12. Cedefop shall be allowed to carry audits or let them carry out by a third party if the service provider (and all its (sub-)subcontractors) has the necessary technical and organisational measures in place, has the necessary competences and the efficiency of the control measures including vulnerability and penetration testing based on a commonly agreed audit plan.
- 2.7.13. Cedefop has the right to verify or let verify by a third party, at any moment, the storage, location and access rights of its data and the technical environment on which its data is treated.
- 2.7.14. Communications between the service provider and Cedefop as well between data centres should be encrypted. If possible data "at rest" should also be encrypted.
- 2.7.15. The service provider is not allowed to link Cedefop data and that of its users with other services as geolocalisation, profiling, etc of users and/or data.
- 2.7.16. The service provider has an obligation to inform Cedefop, within 24 hours, of any cyberattaque he was subject to, indicating which Cedefop data was or potentially accessed/modified/copied/made available to non-authorized persons.
- 2.7.17. When the service provider merges or has been taken over by another company the new company must continue, without any delay to guarantee the information and data security measures. If the new company (and its subcontractors) does no longer comply with the information and data security conditions, territory and Patriot act clauses Cedefop has the right to terminate, with immediate effect and without any penalty, the contract. Alternatively, the contractor should immediately change service provider.

Annex K1

- 2.7.18. When the service provider stops its activity (bankruptcy, liquidation, etc) Cedefop's data will be transferred, without any delay, in a common agreed format to another compliant service provider without any costs for Cedefop.
- 2.7.19. At the end of the contract the service provider (and all of its (sub-) subcontractors), after having transferred all Cedefop data back to Cedefop, he is obliged to destroy in a secure and irreversible way all Cedefop data (including backups, temporary files, previous versions and file fragments) within a commonly agreed time period.
- 2.7.20. The successful tenderer is obliged to duly complete the Privacy Level Agreement (see Annex K3), in coordination with Cedefop and after signature of the contract.

2.8. Support

- 2.8.1. The contractor shall provide 1st and 2nd level support services for a limited number of content editors (Working hours: 09:00 to 19:00 time zone GMT+2).
- 2.8.2. The contractor shall use an automated tool for the registration, management and reporting of support requests (issue tracking system). Incident requests and change requests should both be handled by the same tool. Cedefop is using JIRA as issue tracking system. The tenderer is however free to propose another equivalent system.
- 2.8.3. The contractor shall provide the means for Cedefop staff to report new support requests both inside and outside of the stated working days and hours (Monday to Friday, 09:00 to 19:00 time zone GMT+2).
- 2.8.4. The contractor shall provide the necessary support and ensure that support requests and incidents are addressed as follows:

	Average response time to open support ticket	Maximum resolution times to resolve incident (reported by Cedefop during working hours)
Low priority	16 working hours	3 working days
Medium priority	4 working hours	2 working days
High/Critical priority	1 working hour	4 working hours

The resolution time is the elapsed time between the contractor responding to a support ticket opened by Cedefop and the contractor successfully resolving the Incident.

These resolution times are applicable specifically to incidents identified by Cedefop.

Annex K1

Critical issues related to failures at the server or network level should be monitored and resolved proactively by the contractor.

2.8.5. The contractor shall have incident management policies and procedures in place that describe how problem/issue escalation is handled and measured.

2.9. Administration

2.9.1. The contractor shall apply, throughout the duration of the contract, server system administration policies and procedures including software upgrade and patch application, capacity monitoring/management and change control .

2.9.2. In exceptional circumstances, major software upgrades may make the object of a separate order form.

2.9.3. The contractor shall apply, throughout the duration of the contract, server system administration policies and procedures that govern the backup/restore processes, including backup tools used, retention cycles and policies, frequency, restore procedures, backup validation procedures, and off-site storage facilities and processes .

3. MONITORING/REPORTING

The Contractor shall provide monthly reports to be submitted on the hosting, support and maintenance of Cedefop systems. The reports to be delivered will document at least the following information, for the current month and cumulatively since the beginning of the current year, wherever applicable:

- Scheduled downtimes of the public site and CMS
- Non-scheduled downtimes of the public site and CMS, and list of incidents
- Server connectivity - monthly traffic report, inbound and outbound
- List of actions which were performed as part of regular maintenance
- Software components: list of changes made in maintenance period
- Issues / Risks: narrative of any issues/risks identified by the contractor.

4. WEB ANALYTICS PACKAGE

The contractor should manage the web analytics package that allows Cedefop to examine the website statistics. The Skills Panorama uses Google Analytics to collect and analyse the relevant quantitative data and metrics such as number of visits, unique visitors, sessions, page-views etc.

The package should be configured to exclude from the reported statistics:

- traffic and downloads made from inside Cedefop (exclude by IP addresses)
- traffic and downloads made by search engine spiders and robots
- partial file downloads (e.g. PDF page views).

Annex K1

Specific Cedefop staff members should be able to login remotely to the web analytics package to view the web statistics and configure reports and alerts. The web analytics software should be such as to cover the needs, services and requirements as described in section 2.6.2 of the main Call for Tenders text.