075637/EU XXVIII. GP
Eingelangt am 04/06/26

Council of the European Union

Brussels, 4 June 2026
(OR. en)

10104/26
ADD 1

Interinstitutional File:
2026/0138 (COD)

TELECOM 292
CYBER 271
MI 587
COMPET 700
IA 150
CODEC 1090

PROPOSAL

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
date of receipt:	3 June 2026
To:	Ms Thérèse BLANCHET, Secretary-General of the Council of the European Union
No. Cion doc.:	COM(2026) 502 annex
Subject:	ANNEX to the Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing a framework of measures for strengthening Europe's cloud and AI ecosystem (Cloud and AI Development Act)

Delegations will find attached document COM(2026) 502 annex.

Encl.: COM(2026) 502 annex

www.parlament.gv.at

EUROPEAN
COMMISSION

Brussels, 3.6.2026
COM(2026) 502 final

ANNEXES 1 to 3

ANNEXES

to the

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

establishing a framework of measures for strenghtening Europe's cloud and AI ecosystem (Cloud and AI Development Act)

{SEC(2026) 502 final} - {SWD(2026) 502 final} - {SWD(2026) 503 final}

www.parlament.gv.at

ANNEX I

GRAND CHALLENGES

1. Grand Challenge 1: Environmental sustainability, performance and security of the Union's data centres

Testing and deploying technologies for data centres across the Union to surpass state-of-the-art energy-efficiency and resource efficiency.

This includes achieving lower Power Usage Effectiveness (PUE) and enabling significantly higher server utilisation rates. Examples include:

(1) ***Lowering average Power Usage Effectiveness***: improving the environmental sustainability and performance of the Union's cloud and edge data centres to an average Power Usage Effectiveness (PUE) of 1.15 across the Union. The main focal areas include enabling the development of:

(a) advanced data centre energy efficiency technologies such as cooling, waste heat recovery;

(b) quantum computing technologies for cloud and compute infrastructure operations;

(c) grid integration and advanced energy management systems;

(d) pilot lines for the validation of next-generation energy-efficient technologies at operational scale.

(2) ***Raising average server utilisation rates of data centres:*** raising average server utilisation rates across the Union's data centres towards 50%, by integrating for example, AI-powered technologies for dynamic server utilisation management, runtime workload management and scheduling or for balancing utilisation, energy cost, thermal constraints, and latency requirements.

(3) ***Enhancing the security and resilience of data centres:*** enhancing the security and resilience of data centres' value chain and supply by integrating semiconductor technologies and quantum technologies designed and manufactured in the Union, and by improving their resistance to physical and cybersecurity threats, including targeted attacks.

2. Grand Challenge 2: Cloud stacks

Building end-to-end hardware and software cloud stacks, including AI tools, infrastructure, services and management layers to bridge the Union's critical capacity gaps.

This includes building AI servers powered by semiconductors and quantum technologies designed and manufactured in the Union for distributed and decentralised cloud and edge computing for AI.

Pilot programmes could help demonstrate the capabilities of the European open cloud stacks in strategically important sectors.

3. Grand Challenge 3: Frontier AI

Developing the next generation of multimodal frontier AI models and systems and pioneering novel capabilities.

The focus will be on the architectural design and development of next-generation multimodal models and systems that push the boundaries of current algorithmic capabilities for achieving superior performance in advanced reasoning, cross-modal understanding and agentic

www.parlament.gv.at

capabilities; investigating novel approaches to model efficiency, cognitive modelling, and alternative computational structures, etc.

The potential applications could include foundational science such as scientific discovery and complex data interpretation, and the development of world models for improved reasoning, automated management simulation and planning.

4. Grand Challenge 4: Physical AI

Developing advanced physical AI models and systems that operate autonomously and safely for delivering robust, manipulation and navigation in unstructured environments.

The focus will be on co-designing software and its underlying hardware architectures and on combining frontier AI techniques with world models supporting physical reasoning for delivering robust manipulation, navigation, and interaction capabilities with minimal human supervision.

The potential applications could include autonomous robots, industrial systems and drones operating in dynamic real-world environments.

5. Grand Challenge 5: Industrial AI

Accelerate the development and deployment of European industrial AI across the Union's strategic sectors.

The focus will be on developing European industrial AI models and systems capable of serving high-value industrial applications. Such models and systems should be adaptable to sector-specific use cases and enable secure deployment.

The initiatives launched under this grand challenge should rely on specialised computing resources and testing facilities necessary to validate AI systems in real-world environments before supporting their large-scale deployment and uptake, including at regional and local level.

In the automotive sector, those initiatives may facilitate the development and deployment of innovative software platforms and AI models for automated driving, while in manufacturing, they may enable the creation of specialised models that optimise production processes. Other strategic sectors that could benefit from industrial AI may include healthcare, energy, agri-food and defence.

6. Grand Challenge 6: Cooperative European Industrial Models

Developing cooperative European industrial AI models and systems for strategic sectors by enabling collaboration at European industrial scale without exposing commercially sensitive data between participants.

The focus will be on advanced confidentiality-preserving technologies. Those mechanisms include federated and distributed training approaches where algorithms are brought to the data rather than data being transferred centrally; secure execution environments, encryption-based processing, anonymisation and pseudonymisation techniques, access compartmentalisation, and protections against the extraction of commercially sensitive information from trained models.

Strategic sectors that could benefit from cooperative European industrial AI models and systems may include aerospace, pharmaceutics, cybersecurity, mobility, autonomous vehicles and drones, energy and defence.

www.parlament.gv.at

7. Grand Challenge 7: AI Agents Platform

Developing a European AI agent orchestration framework, providing the essential middleware for the resilient and secure deployment of autonomous agents at scale.

The focus will be on (i) exploring innovative technological paradigms that enable multiple AI agents to collaborate effectively, surpassing the capabilities of standalone systems while maintaining rigorous security standards; and (ii) on the creation of resilient, cloud-based open platforms dedicated to the large-scale management of AI agents.

The potential applications could include healthcare (such as clinical decision support and research coordination), cybersecurity (such as threat detection and response), as well as foundational science.

8. Grand Challenge 8: Public Sector AI

Developing AI models and systems, based on high-quality data from the public sector targeting critical domains (such as healthcare, public administration, law and crisis management as well as public services)

The focus will be on public service solutions that are expected to have a high positive impact on the most critical public services and are shared across different levels of public sector organisations.

One target will be to enable data sharing and frontier model development across national public services to increase the impact on the overall Union's public sector, including also in areas handling sensitive data. Privacy-preserving frameworks, (such as federated learning and high-fidelity synthetic data generation), that make it possible to train of models without compromising the confidentiality of underlying datasets, and measures to accelerate the broad uptake of those modems, including at regional and local level, will also help achieve this target.

www.parlament.gv.at

ANNEX II

CRITERIA FOR UNION ASSURANCE LEVELS

This Annex sets out the criteria to be met by cloud computing service providers and their cloud computing services in order to be recognised as offering services at Union assurance levels 1, 2, 3 and 4. For the purpose of the criteria under Union assurance levels 1, 2, 3, and 4, 'software' within the meaning of Regulation (EU) 2024/2847, Article 3, point (4) falls within the scope of this Annex and Annex III to this Regulation. 'Hardware' within the meaning of Regulation (EU) 2024/2847, Article 3, point (5) is outside of the scope.

1. Union assurance level 1

1.1. For Union assurance level 1, cloud computing service providers must meet the following cumulative criteria:

(a) the cloud computing service provider is established in the Union;

(b) the infrastructure and assets of the cloud computing service provider, including those of its subcontractors which are involved in the provision of the service, are located in the Union unless the public sector body explicitly requires otherwise;

(c) the customer data, including metadata and telemetry data, that is processed, stored and transferred by the cloud computing service provider, and by the subcontractors, which are involved in the provision of the service, remain exclusively within the Union, unless the public sector body explicitly requires otherwise and at any time, including before, during or after the configuration or use of the service;

(d) where the cloud computing service provider outsources the technical and operational support or assistance, including any subsequent sub-outsourcing arrangements, to third-party service providers outside of the Union, the necessary legal, technical and organisational measures are implemented to ensure traceability, security and governance of those operations and those operations do not, in any way, compromise the operational autonomy of the cloud computing service provider;

(e) the cloud computing service provider demonstrates that the service complies with the state-of-the-art cybersecurity standards;

(f) the cloud computing service provider provides full transparency around the use of subcontractors. The cloud computing service provider subjects subcontractors to due diligence, contractual obligations and ongoing oversight to meet Union legal obligations;

(g) Where the cloud computing service provider is subject to the control of a third country or a legal entity established in a third-country, the cloud computing service provider guarantees that there are no existing laws and practices in that third country, demonstrated by independent sources, that require the cloud computing service provider to report information on software vulnerabilities to authorities of that third country prior to those vulnerabilities being known to have been exploited.

1.2. For Union assurance level 1, the subcontractors referred to in the first paragraph must be subcontractors that are third parties that have a direct contractual relationship with the cloud computing service provider and that contribute to the provision and the delivery of the cloud computing service.

2. Union assurance level 2

www.parlament.gv.at

2.1. For Union assurance level 2, cloud computing service providers must meet the following cumulative criteria:

(a) the audited provider and the subcontractors which are involved in the provision of the audited service are established in the Union;

(b) the infrastructure, assets, and personnel of the audited provider, including those of its subcontractors which are involved in the provision of the service are located in the Union;

(c) the customer data, including metadata and telemetry data, that is processed, stored and transferred by the audited provider and the subcontractors which are involved in the provision of the service, remain exclusively within the Union, unless the public sector body explicitly requires otherwise and at any time, including before, during or after the configuration or use of the service;

(d) if the public sector body determines that imposing additional personnel screening and Union citizenship requirements are necessary, the audited provider should ensure that presonnel meeting those requirements are available;

(e) the audited service obtains a European cybersecurity certificate of at least assurance level 'substantial' under a European cybersecurity certification scheme covering cloud computing services to be established under Regulation (EU) 2019/881, provided that such a scheme has been established under that Regulation and is available to cloud computing service providers. Until the establishment of such a scheme, national cybersecurity certification schemes shall apply, where they exist. Where no Union or national cybersecurity certification schemes exist, the audited provider is to demonstrate that the service complies with the highest cybersecurity standards under applicable Union law;

(f) the data generated by using the audited service are not used to train or fine-tune any AI system operated by a third country or a legal entity established in a third-country , and are not transferred outside the Union in any case;

(g) if the audited provider and the subcontractors which are involved in the provision of the audited service are subject to the control of a third country or a legal entity established in a third-country, they demonstrate that the necessary legal, technical and organisational measures have been implemented to ensure that the:

i. control of the third country or the legal entity established in a third-country over the audited provider is not exercised in a manner that restrains or restricts the provider's ability to perform and deliver the service, imposes limitations on the infrastructure, assets, and personnel required for the service provision, or undermines the capabilities and standards necessary to perform the audited service;

ii. access by a third country or by a legal entity established in a third-country to customer data is prevented;

iii. possibility of disruption of the service continuity and/or the degradation of the service quality by a third country or a legal entity established in a third country is prevented;

iv. control of the third country or the legal entity established in a third-country over the audited provider is not exercised in a manner that obliges the audited provider to implement, enforce, give effect to, or comply with restrictive measures such as sanction regimes, embargoes, or any equivalent legal or

www.parlament.gv.at

administrative measures adopted by a third country, unless such measures are legitimate under the national laws of Member States or Union law

(h) the technical and operational support or assistance related to the audited service, including subsequent sub-outsourcing arrangements, are initiated and performed exclusively within the Union;

(i) the audited provider demonstrates that the following software supply chain measures are in place:

i. a complete and up-to-date software bill of materials (SBOM), as defined in Article 3, point (39), of Regulation (EU) 2024/2847,and a list of identified dependencies relevant to the provision of the service are documented and made available to the auditing organisation;

ii. where software components as defined in Regulation (EU) 2024/2847 Article 3, point 6 or products are provided, owned, and licensed by a legal entity established in a third country, controls are implemented and documented to block any remote features that could materially tamper with or disrupt a device, system, or software (including during updates) and to ensure that the security-relevant components from third-country software manufacturers, as defined in Regulation (EU) 2024/2847 Article 3, point 13, are subject to source code audits, and have a documented migration plan in the event that the vendor fails or a third country imposes restrictions;

iii. where the cloud computing service provider is subject to the control of a third country or a legal entity established in a third-country, the cloud computing service provider guarantees that there are no existing laws and practicesin that third country, demonstrated by independent sources, that require the cloud computing service provider to report information on software vulnerabilities to authorities of that third country prior to those vulnerabilities being known to have been exploited;

(j) where software released under an open-source licence is used for the provision of the service, the audited provider demonstrates that it has implemented and documented the appropriate controls to prevent the use of any remote features or mechanisms that could be used to materially tamper with or disrupt a device, system, or software;

(k) to the extent that the audited provider provides its services globally and maintains a subsidiary in a third country, the audited provider has implemented the necessary measures to ensure and enforce the effective legal, technical and organisational separation between the Union parent company and any such third-country subsidiary.

2.2. For Union assurance level 2, the subcontractors referred to in the first paragraph must be subcontractors that are third parties that have a direct contractual relationship to the cloud computing service provider and that contribute to the provision and delivery of the cloud computing service.

3. Union assurance level 3

3.1. For Union assurance level 3, cloud computing service providers must meet the following cumulative criteria:

(a) the audited provider and the subcontractors which are involved in the provision of the audited service are established in the Union;

www.parlament.gv.at

(b) the infrastructure, assets, and personnel of the audited provider, including those of the subcontractors which are involved in the provision of the service, are located in the Union;

(c) the customer data, including metadata and telemetry data, that is processed, stored and transferred by the audited provider and the subcontractors which are involved in the provision of the service, remain exclusively within the Union unless the public sector body explicitly requires otherwise and at any time, including before, during or after the configuration or use of the service;

(d) the personnel, including the personnel of the subcontractors which are involved in the provision of the audited service are Union citizens and where appropriate, the personnel must also have the necessary national security clearance issued by a Member State when handling classified information, as defined in Article 2, point (21), of Regulation (EU) 2021/697;

(e) the audited service obtains a European cybersecurity certificate of at least assurance level 'substantial' under a European cybersecurity certification scheme covering cloud computing services to be established under Regulation (EU) 2019/881, provided that such a scheme has been established under that Regulation and is available to cloud computing service providers. Until the establishment of such a scheme, national cybersecurity certification schemes shall apply, where they exisit. Where no Union or national cybersecurity certification schemes exist, the audited provider is to demonstrate that the service complies with the highest cybersecurity standards under applicable Union law;

(f) the data generated by using the audited service are not used to train or fine-tune any AI system operated by a third country or a legal entity established in a third-country and are not transferred outside the Union in any case;

(g) the audited provider and the subcontractors which are involved in the provision of the audited service are not subject to the control of a third country or a legal entity established in a third-country. By way of derogation to this criterion, a cloud computing service provider and its subcontractors which are involved in the provision of the audited service that are subject to the control of a third country or a legal entity established in a third-country may be audited for Union assurance level 3 where the Commission has adopted an implementing act under Article 19. Where the Commission has adopted an implementing act under Article 19, the audited provider and the subcontractors which are involved in the provision of the audited service must also demonstrate that the necessary legal, technical and organisational measures have been implemented to ensure that the:

i. control of the third country or the legal entity established in a third-country over the audited provider is not exercised in a manner that restrains or restricts the provider's ability to perform and deliver the service, imposes limitations on the infrastructure, assets, and personnel required for the service provision, or undermines the capabilities and standards necessary to perform the audited service. The audited provider should allow for reasonable access to the code;

ii. access by a third country or by a legal entity established in a third-country to customer data is prevented;

iii. possibility of disruption of the service continuity and/or the degradation of the service quality by a third country or a legal entity established in a third country is prevented;

www.parlament.gv.at

iv. control of the third country or the legal entity established in a third-country over the audited provider is not exercised in a manner that obliges the audited provider to implement, enforce, give effect to, or comply with restrictive measures such as sanction regimes, embargoes, or any equivalent legal or administrative measures adopted by a third country, unless such measures are legitimate under the national laws of Member States or Union law;

(h) the technical and operational support or assistance related to the audited service, including subsequent sub-outsourcing arrangements, are initiated and performed exclusively within the Union, by personnel that are Union residents, and by third parties that are not subject to the control of a third country or a legal entity established in a third country;

(i) the audited provider demonstrates that the following software supply chain measures are in place:

i. a complete and up-to-date SBOM and a list of identified dependencies relevant to the provision of the service are documented and made available to the auditing organisation;

ii. where software components or products are provided, owned, and licensed by a legal entity established in a third country, controls are implemented and documented to block any remote features that could materially tamper with or disrupt a device, system, or software (including during updates) and to ensure that the security-relevant components from third-country manufacturers are subject to source code audits, and have a documented migration plan in the event that the vendor fails or a third country imposes restrictions;

iii. where the cloud computing service provider is subject to the control of a third country or a legal entity established in a third-country, the cloud computing service provider guarantees that there are no existing laws and practices in that third country, demonstrated by independent sources, that require the cloud computing service provider to report information on software vulnerabilities to authorities of that third country prior to those vulnerabilities being known to have been exploited;

(j) where software released under an open-source licence is used for the provision of the service, the audited provider demonstrates that it has implemented and documented the appropriate controls to prevent the use of any remote features or mechanisms that could be used to materially tamper with or disrupt a device, system, or software;

(k) to the extent that the audited provider provides its services outside of the Union and maintains a subsidiary in a third country, the audited provider demonstrates that it has implemented the necessary measures to ensure and enforce the effective legal, technical and organisational separation between the Union parent company and any such third-country subsidiary.

3.2. For Union assurance level 3, the subcontractors referred to in the first paragraph must be subcontractors that are third parties that have a direct contractual relationship to the cloud computing service provider and that contribute to the provision and the delivery of the cloud computing service, and that may require access to classified or sensitive information, as defined in Article 2, point (22), of Regulation (EU) 2021/697.

4. Union assurance level 4

www.parlament.gv.at

4.1. For Union assurance level 4, cloud computing service providers must meet the following cumulative criteria:

(a) the audited provider and the subcontractors which are involved in the provision of the audited service are established in the Union;

(b) the infrastructure, assets, and personnel of the audited provider, including the subcontractors , which are involved in the provision of the service, are located in the Union;

(c) the customer data, including metadata and telemetry data, which, following a risk assessment, is identified as sensitive, that is processed, stored and transferred by the audited provider and the subcontractors which are involved in the provision of the service, remain exclusively within the Union and at any time, including before, during or after the configuration or use of the service;

(d) the personnel, including the personnel of the subcontractors , which are involved in the provision of the audited service are Union citizens and, where appropriate, the personnel must also have the necessary national security clearance issued by a Member State when handling classified information;

(e) the audited service obtains a European cybersecurity certificate of at least assurance level 'high' under a European cybersecurity certification scheme covering cloud computing services to be established under Regulation (EU) 2019/881, provided that such a scheme has been established under that Regulation and is available to cloud computing service providers. Until the establishment of such a scheme, national cybersecurity certification schemes shall apply, where they exist. Where no Union or national cybersecurity certification schemes exist, the audited provider is to demonstrate that the service complies with the highest cybersecurity standards under applicable Union law;

(f) the data generated by using the audited service are not used to train or fine-tune any AI system operated by a third country or a legal entity established in a third-country, and are not transferred outside the Union in any case;

(g) the audited provider and the subcontractors which are involved in the provision of the audited service are not subject to the control of a third country or a legal entity established in a third-country;

(h) the technical and operational support or assistance related to the audited service, including subsequent sub-outsourcing arrangements, are initiated and performed exclusively within the Union, by personnel that are Union residents, and by third parties that are not subject to the control of a third country or a legal entity established in a third country;

(i) the audited provider demonstrates that the following software supply chain measures are in place:

i. a complete and up-to-date SBOM and a list of identified dependencies relevant to the provision of the service are documented and made available to the auditing organisation;

ii. measures in place to retain effective control over the software components or products by demonstrating that a third country or a legal entity established in a third country does not hold or exercise effective control over the design, development, maintenance, and evolution of those components or products. Effective control includes the ability to materially influence the technical

www.parlament.gv.at

evolution, maintenance priorities, security remediation, and long-term continuity of the component;

(j) where software released under an open-source licence is used, the audited provider demonstrates that it has implemented and documented the appropriate controls to prevent the use of any remote features or mechanisms that could be used to materially tamper with or disrupt a device, system, or software;

(k) to the extent that the audited provider provides its services outside of the Union and maintains a subsidiary in a third country, the audited provider demonstrates that it has implemented the necessary measures to ensure and enforce the effective legal, technical and organisational separation between the Union parent company and any such third-country subsidiary.

4.2. For Union assurance level 4, the subcontractors referred to in the first paragraph must be subcontractors that are third parties that have a direct contractual relationship to the cloud computing service provider, that contribute to the provision and delivery of the cloud computing service, and that may require access to classified or sensitive information in order to carry out the service provision.

www.parlament.gv.at

ANNEX III

AUDIT EVIDENCE FOR THE AUDIT PROCEDURE

Auditing organisations should request the audit evidence listed in this Annex from the audited provider when assessing the compliance of the audited service against the applicable audit criteria under Annex II.

This Annex is indicative and does not limit the evidence that may be requested or considered by the auditing organisations. Auditors may seek any additional information necessary to ensure a comprehensive and accurate assessment of compliance to conduct audits. While the evidence requested may be the same, the aspects that need to be analysed will differ depending on the assurance level criteria and their strictness.

1. Audit criterion A – Union establishment

The auditing organisation should assess the audit criterion listed under Union assurance levels 2, 3, and 4 paragraph (a) of Annex II based on the following:

(1) Any evidence demonstrating that the audited provider is incorporated under the law of a Member State in the Union or otherwise constituted in line with company law of a Member State in the Union.

(2) Any evidence that the registered office, central administration, and main establishment of the audited provider is established within the Union.

(3) The auditing organisation should verify the applicable Union legal framework of the audited provider and verify whether their establishment is genuine and stable or whether the audited provider instead qualifies only as a non-EU provider offering services in the Union.

(4) The auditing organisation should verify whether the provider is legally incorporated in a Member State of the Union. Evidence of this could include, but is not limited to, the national company extracts, tax residency documentation, business licences, VAT registration, verification of whether the provider is registered in the Business Registers Interconnected System (BRIS) and the VAT information Exchange System (VIES).

(5) The auditing organisation should verify the stable and effective presence in the Union of the audited provider. The auditing organisation should therefore verify that:

  (a) EU physical offices or operational premises exist (for example, through lease contracts, utility bills or property documents);

  (b) permanent staff is located in the Union and that customer support operations are carried out in the Union (for example, through employment contracts, payroll records, personnel timesheets);

  (c) contractual operations are handled in the Union (for example, through activity management records, incident reporting records);

  (d) banking and accounting functions are exclusively in the Union (for example, through financial statements and statutory audit reports).

(6) The auditing organisation should verify the presence of EU Member State establishment units or branches (for example, through lease contracts, utility bills, property documents, employment contracts, timesheets, payroll records or purchase orders).

www.parlament.gv.at

2. Audit criterion B – Location of infrastructure, assets, and personnel

The auditing organisation should assess the audit criterion listed under Union assurance levels 2, 3, and 4 paragraph (b) of Annex II based on the following evidence:

(1) Location of infrastructure

(a) A list with relevant details of the location of the infrastructure and data storage locations used in the provision of the audited service. This list should include the precise location (number, street, city, postal code and country) of the infrastructure demonstrating that all elements remain within the Union for the provision of the audited service. This includes the location for the primary, backup, disaster recovery and log storage.

(b) Any other evidence that the IT infrastructure is located in the Union such as lease agreements, property deeds, maintenance contracts, service contracts, facility access logs.

(c) Network diagrams and architecture documents illustrating the exclusive use of Union-based infrastructure for data storage and processing, including backup and replicated data.

(2) Location of assets

(a) A list and relevant details of the assets used in the provision of the audited service, such as an asset register.

(b) Evidence that servers, equipment, and operational assets are located in the Union, such as records identifying the server and its location, purchase invoices, delivery notes, licence agreements, subscription contracts, or invoices for software purchases or subscriptions, invoices with delivery proofs for hardware.

(c) Evidence that service delivery capabilities are based in the Union, such as deployment records, installation records, service status reports, configuration reports, monitoring outputs, admin logs showing usage of the service.

(3) Location of personnel

(a) A list and relevant details of the personnel involved in the provision of the audited service.

(b) Evidence that the personnel involved in the provision of the audited service are located in the Union, including employment contracts, payroll records, timesheets, activity records, and organisational charts showing Union-based staff with operational responsibilities.

(4) Considerations regarding the infrastructure, assets and personnel

(a) The auditing organisation should also assess where such infrastructure, assets, or personnel:

i. store, transmit, access, process or otherwise handle customer data;

ii. provide, enable, or could enable administrative access to, control over, configuration of, or visibility into customer data;

iii. if compromised, misconfigured, made unavailable or disrupted could reasonably result in the disruption or unavailability of the audited service.

www.parlament.gv.at

***NB**: 'Infrastructure' means physical infrastructure, including but not limited to, data centre infrastructure or colocation infrastructure, network, cooling, and IT systems that allow for the management of the datacentre.*

'Assets' means hardware and software, including, but not limited to, libraries, the internal network needed for software components to communicate, cryptographic materials that enables the provision of the cloud computing service.

'Personnel', including personnel managed by subcontractors, means individuals who support the delivery, administration, security, availability, or operation of the audited service.

3. Audit criterion C – Data localisation in the Union

The auditing organisation should assess the audit criterion listed under Union assurance levels 2, 3, and 4 paragraph (c) of Annex II based on the following evidence:

(1) Evidence demonstrating that customer data are stored and processed exclusively in the Union and that third-parties or subcontractors that do not meet the conditions under this Annex are in no circumstances technically or operationally able to access, obtain, make unavailable, destroy or more generally process customer data without prior authorisation. Examples include access logs, support access policies, privileged access records, backup retention policy, data flows diagram demonstrating where the customer data are stored, processed, replicated and backed up. When processing personal data, contracts with the subcontractors that demonstrate compliance with Regulation (EU) 2016/679.

(2) Evidence of logs and monitoring records demonstrating that all data are stored and processed exclusively within the Union. Examples include master service agreements, data processing agreements, data residency contractual agreements or any EU data boundary.

(3) Evidence (such as contractual agreements, logs, and procedures offered to public sector bodies) demonstrating that the audited provider and the subcontractors which are involved in the provision of the audited service have put in place the necessary measures to ensure that:

   (a) no customer data, including encrypted data, are transferred outside of the Union without public sector body approval;

   (b) no data are transferred to any third-party other than subcontractors which are involved in the provision of the service or recipients expressly authorised by the public sector body.

(4) A data flow diagram showing the flows of data between the cloud computing service provider and customer data, as well as with third-party services and subcontractors. The diagram must clearly identify the source and destination of data and demonstrate that the data does not leave the Union.

NB: For the purpose of this Annex, a customer means a public sector body who has entered into a contractual or other legally binding arrangement with the cloud computing service provider for the purpose of accessing or using the cloud computing service.

'Customer data' could mean any data under the control of the cloud computing service customer, whether by legal, contractual, or other means, that are:

www.parlament.gv.at

(a) input into the cloud computing service by or on behalf of the customer, including authentication credentials;

(b) produced through the customer's use of the cloud computing service.

Customer data may also include data under the audited providers control that are derived as a result of interaction with the audited service by the cloud service customer. This includes customer data and any data resulting from the usage of the cloud computing services (i.e. telemetry, metadata).

'Cloud compunting service derived data' includes the portion of log data containing records of who used the service, at what times, which functions, types of data involved and so on. It can also include information about the numbers of authorised users and their identities. It can also include any configuration or customisation data, where the cloud computing service has such configuration and customisation functionalities.

4. Audit criterion D – Union citizenship

The auditing organisation should assess the audit criterion listed under Union assurance levels 2, 3, and 4 paragraph (d) of Annex II based on the following evidence:

(1) The audited provider should provide the auditing organisation with proof that it has implemented the measures to ensure that, if a public sector body were to request Union citizenship, the personnel involved in the provision of the audited service are Union citizens. This can be demonstrated through valid official government issued documents (e.g. valid passport and national identity card);

(2) The audited provider should provide organisational charts and job descriptions confirming that it can ensure, where requested, that only personnel with Union citizenship have access to the audited service's operation, management, maintenance, and support.

(3) The audited provider should provide documents demonstrating access control policies and audit trails showing that only authorised personnel who are Union citizens can access the service's systems and data.

(4) The audited provider should demonstrate that it has put in place procedures describing how citizenship is verified before assignment and how compliance with this audit criterion is maintained throughout employment.

***NB:** Personnel involved in the provision of the audited service could include personnel who have logical or physical access to infrastructure and assets used to operate the cloud computing service, as well as those who are responsible for customer support, and all personnel who have management control of the cloud compunting service provider.*

5. Audit criteria E – European cybersecurity certification scheme adopted under Regulation 2019/881

The auditing organisation should assess the audit criterion listed under Union assurance levels 2, 3, and 4 paragraph (e) of Annex II based on the following evidence:

(1) A valid European cybersecurity certificate issued by a competent conformity assessment body demonstrating that the audited service has been assessed and found compliant with the requirements corresponding to the 'basic', 'substantial' or 'high' assurance levels under a European cybersecurity certification scheme adopted under Regulation (EU) 2019/881, provided that such shas been established ;

www.parlament.gv.at

(2) A certification report including a description of the main components used for the development and operation of the cloud computing service that is covered by the audit certificate.

(3) Until the European cybersecurity certification scheme covering cloud computing services has been established, the audited provider can demonstrate compliance through valid cybersecurity certifications. This can include, but is not limited to, the following:

(a) a valid certificate issued by a competent conformity assessment body (in line with CEN/CLC/TS 18072:2025) demonstrating that the cloud computing service has been assessed and found compliant with the requirements corresponding to the 'basic' or 'substantial' or 'high' assurance levels defined under CEN/TS 18026:2024;

(b) A valid certificate issued by the relevant national competent authority demonstrating that the cloud computing service has been assessed and found compliant with the requirements under the national cybersecurity scheme currently in place in the Member State;

(c) in the absence of a national scheme, evidence demonstrating adherence to the highest level of cybersecurity standards available on the market.

6. Audit criterion F – AI systems operated by a third country or third country legal entity

The auditing organisation should assess the audit criterion listed under Union assurance levels 2, 3, and 4 paragraph (f) of Annex II based on the following evidence:

(1) Contractual clauses stating that data processed or generated by using the audited service, including customer-derived data, logs and telemetry, will not be used to train or fine-tune any AI model or system operated by a third country or a third-country legal entity, and are not transferred outside the Union in any case.

(2) Contractual clauses specifying that data are processed solely for the delivery of the audited service and not for service improvements or model or system enhancements or any other secondary purpose.

(3) Data flow diagrams documenting the end-to-end flow of data, covering data ingestion, storage, processing and deletion. The diagrams should also show where the AI pipelines or machine learning operations (MLOps) connect with customer data.

(4) MLOps or deployment records demonstrating that the build, test and release locations are in the EU.

(5) Model or system cards covering the model or system name, version, training and validation sources, including statements that the data generated by using the audited service does not leave the Union.

(6) Data lineage polices and related implementation documentation that shows that the provider operates data lineage and provenance tools and that can demonstrate (per record) what the data has been used for.

(7) A list of the subcontractors (indicating their country of establishment) that access the data generated by using the audited service.

www.parlament.gv.at

7. Audit criterion G – Absence of third-country control or third-country entity control

The auditing organisation should assess the audit criterion listed under Union assurance levels 2, 3, and 4 paragraph (g) of Annex II based on the following evidence:

(1) The auditing organisation should identify and analyse:

(a) all direct and indirect shareholders, up to the ultimate owners;

(b) the cap table documenting the company's ownership structure;

(c) the body or bodies empowered to take strategic decisions (general assembly of shareholders, supervisory board, board of directors, etc.);

(d) the rules for the appointment/election/removal of governing bodies and the actual composition of the governing bodies (e.g. to identify if any shareholder is entitled to nominate a board representative or has majority seats in the board);

(e) the quorums and majority required for adopting strategic decisions, in order to determine if any shareholder can take a strategic decision (either because they have the required majority to approve such a decision or because they can block such a decision through a veto or other specific rights even if they cannot impose such a decision on their own, etc.);

(f) the possible influence on strategic decisions through commercial links, financial links or other means, etc.

(2) The audited provider should request all the above information from its subcontractors and make it available to the auditing organisation.

7.1. Assessment of ownership and control:

(1) The audited provider should provide the auditing organisation with the following evidence related to the headquarters:

(a) the location and full address of the global headquarters and/or head office;

(b) the locations of the executive management structures.

(2) The audited provider should provide the auditing organisation with the following evidence related to the ownership structure and specific rights:

(a) A detailed list describing any owners that:

i. hold, directly or indirectly, at least 5% of the capital or at least 5% of the voting rights, including through any content, understanding, relationship or intermediary. This includes voting agreements between shareholders that would together have more than 5% of the voting rights or 5% of the capital;

ii. have one or more of the following specific rights in relation to their ownership: (a) right to veto a transfer of shares; (b) pre-emption rights; (c) right to purchase additional shares or investment subject to conditions.

(b) The auditing organisation should request the following supporting documents to assess the elements in paragraph 2(a):

www.parlament.gv.at

i. commercial registry extracts and shareholders' books of the organisation and any other relevant document that clearly indicate the shareholders and their voting rights or percentage of interest;

ii. shareholders' agreement, memorandum of understanding among shareholders, statutes, articles of association or other relevant documents regarding the decision-making procedures within the legal entity, investment agreements between the shareholders, etc.;

iii. for any shareholders that are legal persons that hold at least 5% in the capital or at least 5% of the voting rights:

(1) a graph describing the different ownership layers/chain of control until the ultimate owners;

(2) the articles of association, bylaws or equivalent constitutional documents;

(3) a register of directors, officers and signatories.

(3) The audited provider should provide the auditing organisation with the following evidence related to the corporate governance:

(a) The audited provider should provide the auditing organisation with a description of:

i. the decision-making bodies, their composition as well as their nationality or place of establishment (where applicable);

ii. the rules regarding election, appointment, nomination or tenure of members of the decision-making bodies or other management positions;

iii. the decision-making procedures, including information on the required majority and/or quorum needed for decisions;

iv. internal governance policies describing how ownership and control decisions are recorded and approved;

board and management decisions reflecting the stated control structure;

board minutes and resolutions for control changes.

(b) The audited provider should provide the auditing organisation with supporting documents setting out or describing: the decision-making bodies and the rules on their election, appointment, nomination or tenure, decision-making procedures, voting rights, veto rights, appointment rights, approval rights within the legal entity (e.g. articles of association bylaws, reports on corporate governance, etc.). The supporting documents and information should be provided for each intermediate legal entity that directly or indirectly holds 5% or more of the capital or voting rights, up to the ultimate owners of all the layers involved.

(4) The audited provider should provide the following control-related evidence to the auditing organisation:

(a) The audited provider should provide the auditing organisation with the evidence of the commercial links conferring control. This includes, but is not limited to, a list of individuals or legal entities with whom the audited providers (or the owners of the audited provider, including intermediate layers

www.parlament.gv.at

until the ultimate owners) have a commercial relationship that (a) leads to a similar level of control on management and resources as the ownership of shares or assets; and (b) is of very long duration (e.g. very important long-term supply agreements or credits provided by software manufacturers/customers, coupled with structural links).

(b) The supporting documents should include cooperation agreements with the public sector body or software manufacturers , etc.

(5) The audited provider should provide the auditing organisation with the following evidence related to the financial links conferring control:

(a) The audited provider should list the individuals or legal entities (including controlling shareholders or owners) on whom the audited provider (or the owners) are financially dependent in a way that could allow them to obtain concessions in strategic business areas.

(b) The supporting documents should include loan documents, by-laws, documents showing the financial link; etc.

(6) The audited provider should provide the auditing organisation with the following evidence related to other sources of control:

(a) The audited providers should indicate to the audited organisation if there is any other means, process or link ultimately conferring control to another third country or a legal entity established in a third country (similar level of control on management and resources as the ownership of shares or assets and of long duration).

(b) Supporting documents should provide evidence of any such control or a declaration that there is no such control (this declaration may come from the management board of the service provider).

NB: *The elements that should be taken into account when assessing control are the ownership structures and specific rights, corporate governance, commercial links conferring control, financial links conferring control and any other sources of control.*

7.2. Additional steps based on the conclusion of the ownership and control test

If the auditing organisation determines that the audited provider is subject to the control of a third country or a third-country legal entity, it should request the following additional evidence:

(c) Demonstrating that the Commission has adopted a decision pursuant to Article 19 regarding the third country for which the cloud computing service provider is subject to the control of;

(d) All evidence demonstrating that the audited provider and any subcontractorinvolved in the provision of the audited service has implemented the necessary measures to enforce the effective legal, technical and organisational separation between the cloud computing service provider and any third country or legal entity established in a third country, ensuring that the cloud computing service provider is unable to comply, legally, technically and operationally, with any request to access customer data, including encrypted data, or to disrupt service continuity or to degrade service quality.

www.parlament.gv.at

(e) All evidence demonstrating that the public sector body will be informed of any such request and a confirmation that the request has been refused;

(f) All evidence demonstrating the maintenance of an up-to-date record of any request to access customer data, to disrupt service continuity or to degrade service quality from a third country or a legal entity established in a third country, containing at least the request and the response to the request.

8. Audit criterion H – No technical and operational support outside of the Union

The auditing organisation should assess the audit criterion listed under Union assurance levels 2, 3, and 4 paragraph (h) of Annex II based on the following evidence:

(1) evidence that the audited provider has implemented binding contractual clauses stating that all support, administration, maintenance, monitoring, incident response, and operational activities must be initiated and performed exclusively in the Union. This could include contractual clauses requiring advanced disclosure of all subcontractors and support locations, prior written approval before engaging any new subcontractors, and a right to reject any subcontractors located outside of the Union;

(2) evidence that the audited provider maintains an up-to-date subcontractor register;

(3) evidence that the audited provider does not subcontract or transfer such activities outside of the Union;

(4) evidence that the audited provider has implemented the necessary legal, technical and organisational measures to ensure that there can be no remote access for technical and operational support from outside the Union for the audited service.

(5) evidence that the audited provider's help desk/support services, infrastructure administration, operations of its security operations centre (SOC) or network operations centre (NOC), privileged access, backup handling, and disaster recovery operations of the audited service are exclusively provided from the Union, including the access path to operate the service;

(6) evidence that the audited provider ensures that the personnel upon the departure from the company have no further access to the audited service and revokes all access policies;

(7) evidence that the audited provider has implemented the necessary technical and organisational measures to ensure that administrative access to systems used to operate the audited service is provided through access paths located within the Union. This can be demonstrated through the implementation of geographically restricted network controls, Union-based administrative infrastructure, privileged access management controls, and monitoring mechanisms;

(8) evidence that the audited provider has procedures in place that there is no effective control of a third country or a legal entity established in a third country, including for subsequent sub-outsourcing.

9. Audit criterion I - Ensuring the transparency of the software supply chain

The auditing organisation should assess the audit criterion listed under Union assurance levels 2, 3, and 4 paragraph (i) of Annex II based on the following evidence:

(1) The audited provider should make available to the auditing organisation a complete and up-to-date software bill of materials (SBOM) for all software components, including open-source software (OSS).

www.parlament.gv.at

(2) The audited provider should make available to the auditing organisation a list of dependencies. This should include:

(a) all software modules, libraries or application programming interfaces (APIs) used, as well as development tools;

(b) origin of software: where (country of origin) and by whom the software is designed, developed and maintained, the location and jurisdiction governing the software distribution, and updates;

(c) degree of reliance on non-EU vendors, facilities, or proprietary technologies; for level 3, evidence that in case the software stack is provided by a third coutnry entity, no unduly unjustified licensing restrictions are in place.

(d) degree of reliance on open-source software;

(e) visibility into the entire software manufacturer and sub-manufacturer chain, including audit rights.

N.B. *The requirements above imply that joint ventures made, e.g., of a Union entity with a legal entity established in a third country can qualify for this level*

(3) The audited provider should provide:

(a) evidence of a risk-based process for identifying and mitigating dependencies on external software manufacturers relevant to the operation of the cloud computing service;

(b) evidence that it has identified one or more alternative software solutions, including open-source software. If equivalent software cannot be identified, a solution ensuring minimal viable functionality must be identified. Tests must be implemented and a switchover plan enabling migration to such alternative solutions;

(c) evidence that it can migrate to an alternative solution in the event of any defect or failure of the vendor or restrictions from a third country or a legal entity established in a third country;

(d) provide a list of open standards that are followed as part of the audited providers policies regarding the audited service;

(4) The audited provider should ensure transparency through remote access and source code auditability by:

(a) making available to the auditing organisation a list of evidence to prove that there is no use of any remote features or mechanisms that could be used to materially tamper with or disrupt a device, system, or software. This should include:

i. evidence related to the testing of the software component to prevent the use of any remote features or mechanisms that could be used to materially tamper with or disrupt a device, system, or software (test procedure, test reports, test plan, etc.);

ii. evidence that the organisation’s change management procedures cover any change in firmware, bios and software updates as well as integration of a new components to prevent the use of any remote feature or mechanism;

www.parlament.gv.at

iii. evidence that the maintenance procedure is updated to include preventing any remote feature or mechanism that could be used to materially tamper with or disrupt a device, system or software.

(b) The audited provider must ensure that the third-party independent auditor is granted the right to access and audit the source code of such software. The audited provider must also ensure that all documentation, technical material, information necessary to evaluate and audit the source code are made available to the auditing organisation in a complete, accurate, and accessible format.

10. Audit criterion J – Open-source software

The auditing organisation should assess the audit criterion listed under Union assurance levels 2, 3, and 4 paragraph (j) of Annex II based on the following evidence:

(1) The audited provider should ensure transparency through remote access and source code auditability by:

(a) making available to the auditing organisation a list of evidence to prove that there is no use of any remote features or mechanisms that could be used to materially tamper with or disrupt a device, system, or software. This should include:

i. evidence related to the testing of the software component to prevent the use of any remote features or mechanisms that could be used to materially tamper with or disrupt a device, system, or software (test procedure, test reports, test plan, etc.);

ii. evidence that the organisation's change management procedures include any change in firmware, bios and software updates as well as integration of new components to prevent the use of any remote feature or mechanism;

iii. evidence that the maintenance procedure is updated to include preventing any remote feature or mechanism that could be used to materially tamper with or disrupt a device, system or software;

(2) The audited provider should provide:

(a) evidence of a risk-based process to identify and mitigate: (i) a weak ecosystem and community support of the OSS; (ii) a failure to continuously monitor the updates released; (iii) cases where the OSS is deprecated or is no longer maintained.

(b) evidence that the audited provider has applied the up-to-date OSS without undue delay;

(c) evidence that the audited provider has identified one or several alternative open-source solutions. If the audited provider cannot identify an equivalent software, it must identify a solution ensuring minimal viable functionality. The audited provider must implement tests must and a switchover plan enabling migration to the alternative solutions.

(3) Where the audited provider uses software released under an open-source licence, the audited provider should implement mechanisms to detect and provide timely notice to the public sector body if the software is acquired by or comes under control of a third country or a legal entity or foundation established in a third country.

www.parlament.gv.at

11. Audit criterion K – Global services and subsidiaries in third-countries

The auditing organisation should assess the audit criterion listed under Union assurance levels 2, 3, and 4 paragraph (k) of Annex II based on the following evidence:

(1) The auditing organisation should verify that the subsidiary is legally and operationally independent from the audited provider.

(2) The audited provider must demonstrate that the subsidiary has no access to systems processing or storing the customer data.

(3) The audited provider must demonstrate that the subsidiary has no privileged accounts within the Union production environments, including cloud administration, Identity and Access Management (IAM), Privileged Access Management (PAM), monitoring or database administration privileges.

(4) The auditing organisation should verify that the personnel of the subsidiary cannot obtain access to Union customer data.

(5) The auditing organisation should verify that the subsidiary has no authority to instruct Union operational staff to disclose customer data or bypass security procedures.

(6) The auditing organisation should verify that all foreign government requests received by the subsidiary are formally redirected to the competent Union entity for legal assessment under Union and Member State law.

www.parlament.gv.at