

EUROPEAN ALLIANCE FOR INDUSTRIAL DATA, EDGE AND CLOUD

TERMS OF REFERENCE

1. BACKGROUND

As data is becoming a strategic asset to any organisation, cloud and edge technologies are becoming a critical infrastructure underpinning the digital transformation of our society and economy. For this reason, they constitute a priority area for investment and reforms by the EU and its Member States for the coming years and integrate the key targets against which the Commission will assess Europe's digitalisation.¹

As highlighted in the European Strategy for Data², the volume of data generated is greatly increasing and a significant proportion of data is expected to be processed at the edge (80% by 2025, from only 20% today), closer to the users and where data are generated. This shift represents a major opportunity for the EU to strengthen its own cloud and edge capacities, and hence its technological sovereignty.

It will require the development and deployment of fundamentally new data processing technologies, encompassing the edge, moving away from fully centralised data processing infrastructure models. Computing capabilities will increasingly be orchestrated by data management engines based on artificial intelligence. Security will of course remain essential but will become more automated and intelligent, allowing self-configuring and self-healing infrastructures. Highly distributed cloud and edge powered by artificial intelligence will also support the dynamic creation of novel sector-specific and context-sensitive data services. A new paradigm of truly adaptive hybrid computing, multi-vendor and cognitive cloud & edge will emerge.

While the increasing adoption of cloud and edge technologies will spur innovation across the economy and ensure seamless provision of high quality services by public authorities, there is a need for highly secure, fair, trustworthy and competitive cloud and edge capacities. In her State of the Union address, the President of the European Commission stated that Europe should ensure its digital sovereignty, based on clear goals and principles. In this regard, the President put special emphasis on a 'European Cloud'.

When European businesses currently use cloud services, they have little choice but to purchase services offered by non-European entities³, which means that the value of industrial and public sector data is mostly extracted outside Europe. As referenced in the EU's 'Digital

¹ COM(2021)118 final

² COM(2020)66 final (Data Strategy)

³ According to Eurostat's data, while improved compared to 2018, only 36% of EU enterprises used cloud services in 2020, mostly for simple services such as e-mail and storage of files (only 19% of enterprises use advanced cloud services).

Decade’ Communication⁴, this can bring risks in terms of cybersecurity, supply vulnerabilities, switching possibilities as well as unlawful access to data by third countries.⁵

Not only does this put sensitive European (personal, public sector and commercial) data at risk, but it also means that cloud adoption in Europe remains slow, partly because of lack of trust. In particular, where personal data, **sensitive personal data**⁶, **commercially sensitive**⁷ or **highly sensitive public sector data (e.g. defence, security, mobility)** is involved, users expect a high level of assurance regarding compliance with the EU rules⁸ and against (over)dependencies on non-EU service providers.

To address these challenges and attain the objective of a ‘European cloud’, the Alliance will bring together businesses interested to (co-)invest in European solutions and provide a platform for information and identification of synergies across EU and Member States investment programs in the area of cloud and edge, such as the Digital Europe Program, Connecting Europe Facility 2, European Defence Fund and the Recovery and Resilience Facility. This should create the momentum for European industry to invest and strengthen the EU’s position on the next generation of cloud and edge technologies. Participation in the Alliance should also serve to assist emerging providers of cloud services to overcome difficulties to scale-up at European and global level, to reach sufficient scale to deliver services and compete effectively on the market.

2. SUBJECT MATTER

The Alliance is entitled **European Alliance for Industrial Data, Edge and Cloud** (“the Alliance”).

The Alliance will focus on fostering the joint development and deployment of **next generation EU native cloud and edge technologies** that meet the requirements to process Europe’s personal data, sensitive personal data and/or highly sensitive business and public sector data sets, by addressing use cases for all sectors of the economy, with a specific focus on defence, security, mobility, health, and space.

In line with the EU data strategy, these data processing technologies should ultimately underpin the development of **European data spaces**, which are also covering multiple sectors of the economy. To offer full reassurance on the standards and requirements of data processing infrastructures in Europe, the Alliance will further serve as one of the consultation platforms for defining the **EU Cloud Rulebook** and provide expertise on common standards and requirements for the public procurement of cloud services, as foreseen in the European Data Strategy.

⁴ ‘2030 Digital Compass: the European way for the Digital Decade’, <https://eur-lex.europa.eu/legal-content/nl/TXT/?uri=CELEX%3A52021DC0118>

⁵ The EU is acting to mitigate such concerns through mutually beneficial international cooperation, such as the proposed EU-U.S. Agreement to facilitate cross border access to electronic evidence.

⁶ As defined in Article 9 of the Regulation (EU) 2016/679 (General Data Protection Regulation).

⁷ As per Recital 15 of the Data Governance Act proposal, COM(2020) 767 final

⁸ ENISA, the EU Cybersecurity Agency, is developing a proposal for an EU cybersecurity certification scheme for cloud services, including an assurance level “high” for mission critical data: <https://www.enisa.europa.eu/news/enisa-news/cloud-certification-scheme>

3. TASKS

The main task of the Industrial Alliance will be to bring together a wide range of stakeholders that are prepared to work together and advance towards achieving the key objective to strengthen EU's position on the next generation of cloud and edge technologies.

The Alliance will complement other forms of research, commercial and policy cooperation, consultation and exchange in the field, among different constellations of actors. The EU market is among the most open in the world, and the tasks of the Alliance shall in no way affect access to the EU market, whether through sales or establishment, or to EU or national funding - these remain governed by EU law (including programme conditions, State aid rules, international trade commitments, etc.) and national law where applicable.

The Alliance shall:

(1) **leverage investment synergies** by industry for joint development and deployment of the next generation of European cloud and edge technologies that meet the needs of European businesses and public sector dealing with sensitive personal, and highly sensitive business and public sector data. As such, the Alliance could supply detailed recommendations (e.g. use cases; strategic technology and investment roadmaps; market analysis and value chain gaps) and serve as “matchmaking” platform for businesses from different EU Member States;

(2) provide a **platform to create synergies with Common European Data spaces**, in particular those hosting sensitive public sector and business data with high security requirements, gathering the technical requirement for cloud/edge infrastructures and services for those sectors, and ensuring synergies and interoperability among the different data spaces in close coordination with the Support Centre for data sharing and the European Data Innovation Board.

(3) To offer full reassurance on the standards and requirements of data processing infrastructures and services in Europe, the Alliance will further serve as one of the **consultation platforms in the context of the preparatory work of the EU Cloud Rulebook**, and provide expertise on common standards and requirements for the public procurement of cloud services, as foreseen in the European Data Strategy, as part of consultation processes of the Commission open to all stakeholders. **It will also provide a platform for coordination between the Commission and all Member States' public authorities** including on common specifications for public procurement of data processing services, including in fields with a high level of security requirements;

While performing these tasks, the Alliance and its members shall comply fully with EU law and relevant Member State laws, including in the field of competition. In this regard, members of the Alliance shall also subscribe to the **competition compliance programme**, as referenced in Annex to the Alliance Declaration.

4. TECHNOLOGY FOCUS

In line with the objectives of the European Data Strategy and the Industrial Strategy, the activities of the Alliance need to focus on strengthening Europe's industrial position in the global cloud and edge computing market. Therefore, it should specifically address the trend towards increasing **distribution and decentralisation of data processing capacities across of the computing continuum**⁹ and promote an alternative European model to the offerings of cloud hyperscalers. Its ambition should be to meet the highest standards in terms of data

⁹ Future Cloud Research Roadmap Update – August 2020

protection, security, climate neutrality and resource efficiency, interoperability and portability. In particular, the Alliance will focus on following technological challenges:

- **Edge and fog technologies** are still in their infancy and need to be deployed across the EU in a highly secure, energy-efficient manner, including micro/edge data centres.
- The development of **European sovereign cloud stack**, with intelligent middleware enabling the seamless processing of data across different computing environments; this will allow native and complete interoperability across different European infrastructure and service providers, reducing the costs overhead of complex interfaces¹⁰.
- The combination of edge and cloud computing exacerbates the challenges associated with resource management in the cloud, and calls for novel open source **multi-cloud management services** enabling seamless integration of heterogeneous cloud environments of different service providers in a vendor-neutral manner¹¹.
- Novel methods for managing highly-distributed intelligence with embedded self-healing and resilience at large scale, such as **swarm computing** or **empowered edge**, will enable the exploitation of computing capacities in highly heterogeneous hardware environments (edge devices and wide diversity of IoT devices).
- **Computing continuum technology** compatible with the management of hardware heterogeneity, will allow for optimal workload management at the far edge and edge (from smart devices at the far edge to edge to cloud to high performance computing). It will also open new ways towards energy aware, optimised and sustainable edge and swarm computing services¹².
- **New edge and swarm computing scenarios** will need to cater for highly-distributed intelligent collaboration, self-organisation, self-management and self-healing at large scale across many and heterogeneous computing resources present in all kinds of IoT edge devices, micro edge data centres, private enterprise clouds, federated cloud models and large cloud set-ups.
- **Innovative cloud and edge security solutions ensuring trust in the management of sensitive personal or highly sensitive public sector and business data. New state-of-the-art cyber controls, tools & security architecture** will have to be developed addressing the security needs triggered by the adoption of novel applications, supporting the cloud – edge continuum¹³.
- **State of the art solutions for national public sector cloud** will have to be deployed through smart procurement strategy in order to enhance the digitisation of administration & public authorities as well as solutions of e-government, including in fields with a high level of security requirements.
- **Cutting-edge climate-neutral, highly energy-efficient and sustainable technology and edge solutions for efficient infrastructures for data storage and processing**

¹⁰European industrial technology roadmap for the next generation cloud-edge offering, 7 May 2021: <https://digital-strategy.ec.europa.eu/en/library/today-commission-receives-industry-technology-roadmap-cloud-and-edge>

¹¹ [Future Cloud Research Roadmap Update](#), Ibid.

¹² Ibid.

¹³ European industrial technology roadmap for the next generation cloud-edge offering, Ibid.

will position Europe as a leader on the path towards reaching climate neutral data centres by 2030¹⁴. The distributed nature of edge cloud infrastructure will enable a smarter distribution of data across the network thanks to cognitive cloud. This effort also includes the deployment of advanced technologies for energy and resource efficiency, such as direct liquid or immersive cooling, as well as for the optimization of recycling in the hardware supply chain (data centres equipment, servers, edge nodes...).

5. CONSULTATION

Beside the above-mentioned tasks, the Commission may consult the Alliance on other matters relating to policies related to the technology focus described above, or more generally relating to industrial data, cloud and edge. The Alliance may be consulted as part of public consultations launched by the Commission to all stakeholders.

6. MEMBERSHIP ELIGIBILITY CRITERIA

The investment planning synergies being leveraged in the framework of the Alliance shall be completely without prejudice to the legal framework of EU's funding instruments.

In order to achieve the objective of the Alliance in a manner that is not detrimental to EU interests and ensures technological sovereignty and competitiveness, the following membership eligibility criteria shall apply:

- 1) Membership of the Alliance is designed for legal entities ("Member Organisations"). Membership will not be open to individuals appointed in a personal capacity.
- 2) The Alliance is open to all public and private entities with relevant activities in the area of highly secure, interoperable, energy and resource efficient cloud, edge and data capacities, including companies, associations, trade associations, groupings of companies or other entities engaged in interest representation (whose members are meeting the criteria of the Alliance, set out in paragraph 7), and research and technology organisations, investors, civil society organisations, and representatives of EU Member States, regional and public authorities.
- 3) An organisation's membership of the Alliance will be conditional on the signature of the Alliance's Declaration.
- 4) Member Organisations (and where relevant their constituting parties or members) shall have a legal representative established in the Union.
- 5) A legal entity may become a Member Organisation only if it does not contravene the security and/or public policy interests of the Union (including cybersecurity) and can participate in a way that is of practical utility to the Alliance. For that purpose, it shall provide assurances that it complies with the following criteria (in the form a detailed report attached to the binding Declaration):
 - a) Security of sensitive information and data protection: Candidate Member organisations shall provide a signed commitment under which they provide detailed information establishing unequivocally that, in the fields subject to the work of the Alliance, they comply with EU and national rules on protection of personal data,

¹⁴ Ibid.

sensitive personal data, commercially sensitive or highly sensitive public sector personal or non-personal data (e.g. defence, security, mobility), and that they have put in place all reasonable technical, legal and organisational measures in order to prevent transfer or access – including unsolicited transfers or access - to personal or non-personal data (including processed data and meta-data) held in the Union that would be unlawful under Union law or applicable national law. They shall not provide any information related to the Alliance and related projects to third parties, except general information about the Alliance’s work that may be disseminated to non-members exclusively upon specific request of the European Commission.

- b) Security of supply: control over the legal entity by a third country, acting either directly or by way of measures addressed to a third country entity, does not undermine the legal entity’s freedom to use its infrastructure, software, services, facilities, assets, resources, intellectual property or knowhow needed for the purposes of the Alliance, or that undermines its capabilities and standards necessary for the Alliance.
- c) Protection of IP: ownership of the intellectual property arising from, and the results of its involvement in the Alliance, such as that attributable to investment activities deriving from synergies identified under the Alliance, will remain within the member during and after terminating its participation to the Alliance, is not subject to control or restriction by a third country, acting either directly or by way of measures addressed to a third-country entity.
- d) Practical utility to the Alliance: the entity shall describe its relevant existing or planned activities in the European Economic Area¹⁵ of practical utility to the Alliance¹⁶, in the fields set out in section 4 (Technology focus) and section 3 (Tasks).

These criteria will be assessed on a case-by case basis by the Commission, on the basis of information provided by the applicant. Such assessment may result in a refusal of the application of a given eligible organisation or its participation rights restricted.

The entities which are not subject to control by a third country, acting either directly or by way of measures addressed to a third country entity, are normally presumed to respect criteria (a) to (c).

- 6) Paragraphs 4 and 5 shall also apply to subcontractors, constituting parties, shareholders of or members of Member Organisations, where these entities would be in a position to access information related to the Alliance.
- 7) Prior to the signature of the Alliance Declaration, Applicants shall provide all relevant information necessary for the assessment of fulfilment of the eligibility criteria to the European Commission. In the event of a change during the membership which might put into question the fulfilment of the eligibility criteria, the relevant legal entity shall inform the European Commission sufficiently in advance, which shall assess whether these eligibility criteria and conditions continue to be met and shall address the potential impact on the organisation’s membership of the Alliance.
- 8) Before joining the Alliance, each candidate Member Organisation shall provide a written commitment that it has and will ensure in the future¹⁷ to have, no conflict of interest¹⁸

¹⁵ EEA countries are understood to be part of the Union for the purpose of this alliance.

¹⁶ This can include, for instance, a demonstrable commitment to contribute to voluntary sharing and developing know-how and IP; or to the opening, enhancement or expansion of a software development centre for cloud/edge; or to establishing a partnership to pilot new green data centre technologies or to increase the capacities of a cybersecurity centre to focus on cloud and data security.

¹⁷ For the period of membership and two years after membership is finished.

whatsoever with the Alliance's objectives or with specific objectives of the working groups.

- 9) Member Organisations who no longer act in accordance with the principles set forth in the Alliance Declaration, or are no longer capable of doing so, upon request of the Commission, shall no longer be invited to participate in any meetings of the Alliance and may be replaced for the remainder of their term of office.
- 10) Without prejudice to membership, the Commission, for instance upon proposal of the Steering Committee, may restrict discussions related to certain essential strategic tasks affecting security interests of the Union, be it in working groups or General Assembly's agenda points, to Member Organisations not subject to control by a third country, acting either directly or by way of measures addressed to a third country entity.

6. GENERAL ASSEMBLY

1. The **European Commission** will act as a facilitator of the Alliance and organise once per year a **General Assembly**.
2. The **General Assembly** of the Alliance will be made up of high-level representatives (e.g. CEOs/Executive board members) of every Member Organisation.
3. The **General Assembly** elects (a) **chairperson(s)** from among its members not subject to control by a third country, acting either directly or by way of measures addressed to a third country entity.
4. The **European Commission** will be an observer to the General Assembly, monitoring progress with a view to its policy and investment agenda and act as a facilitator towards cooperation and engagement of all stakeholders, e.g. by providing secretarial services for the on-boarding of new members.
5. The **General Assembly** shall adopt opinions, recommendations or reports.
6. When adopting opinions, recommendations or reports, the General Assembly shall do so **by consensus**. In the event of a **vote**, the outcome of the vote shall be decided by simple majority of the members. Members who have voted against shall have the right to have a document summarising the reasons for their position annexed to the opinions, recommendations or reports.
7. Member Organisations should designate a high-level representative to the General Assembly and relevant experts to represent them in the working groups of the Alliance.
8. The European Commission or the Steering Committee may invite Member States representatives to participate in the General Assembly of the Alliance.

7. ALLIANCE FORUM

1. The European Commission will organise an **Alliance Forum**.
2. The Alliance Forum will be an inclusive, transparent and open platform to ensure communication and exchanges between the European Commission, Alliance members and all other stakeholders with an interest in the fields of work of the Alliance.

¹⁸ This involves any actual, potential and perceived conflict of interest.

3. It is aimed at broadening the perspective, making the links with all relevant actors, including globally, and including the views of a wide range of stakeholders.

8. STEERING COMMITTEE

1. The Steering Committee is composed of a balanced group of representatives of Members Organisations, not subject to control by a third country, acting either directly or by way of measures addressed to a third country entity, including SMEs.
2. Members of the Steering Committee are appointed by the European Commission on the basis of Members Organisations' proposals.
3. The Steering Committee prepares the General Assemblies and supports the European Commission in facilitating and monitoring the work of the Alliance.

9. WORKING GROUPS

1. The **General Assembly or the European Commission** may establish working groups of the Alliance, working on specific topics. As a priority, it shall consider the establishment of the following working groups:
 - a. A working group on **investments** for joint development and deployment of the next generation of European cloud and edge technologies that meet the needs of European businesses and the public sector dealing with personal data, sensitive personal data or highly sensitive business and public sector data;
 - b. A working group providing advice to the Commission on the **EU Cloud Rulebook**;
 - c. A working group for Member States public authorities only regarding common specifications for **public procurement of cloud services**, including in fields with high security requirements;
 - d. A working group working on a **strategic cloud and edge technologies roadmap**, which should be regularly updated after the first version is made available;
 - e. A working group **on cloud for defence and security**, which should look at the specific needs of these sectors demanding highest security requirements.
2. Member Organisations wishing to participate in such working groups will designate specific representatives for cooperation in the working groups.
3. Each working group shall elect a Chair and Vice Chair(s) from among representatives of the Members Organisations not subject to control by a third country, acting either directly or by way of measures addressed to a third country entity.
4. Observers and their representatives may be permitted by the Chair, with the agreement of the Commission, to take part in the discussions of the group and provide expertise. However, they shall not have voting rights and shall not participate in the formulation of recommendations or advice of the group.
5. The Commission reserves the right to act as an observer to all working groups of the Alliance.
6. Member States representatives are invited to participate in the work of the Alliance in relevant working groups, in particular those between the Commission and Member States

public authorities related to common specifications for public procurement of data processing services.

10. RULES OF PROCEDURE

The General Assembly of the Alliance shall adopt its rules of procedure by simple majority of its members.

11. PROTECTION OF PERSONAL DATA

The European Commission DG CONNECT will publish on the Register a privacy statement providing information about the processing and the protection of personal data.

The European Commission is committed to protect personal data and to respect privacy. The European Commission collects and further processes personal data pursuant to Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data.

Done in Brussels, on 15 July 2021.