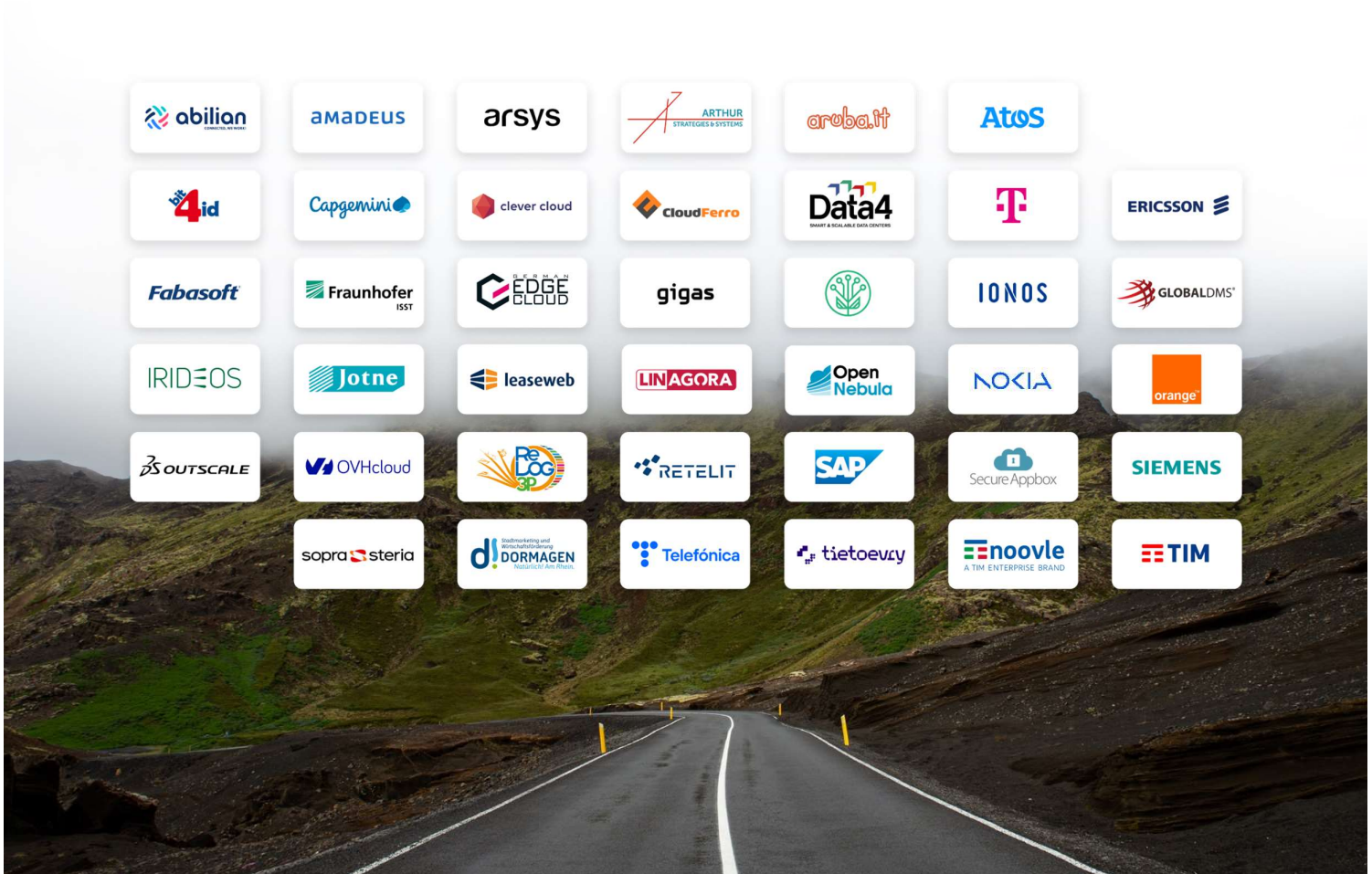
EUROPEAN ALLIANCE
FOR INDUSTRIAL DATA,
EDGE AND CLOUD

# EUROPEAN INDUSTRIAL TECHNOLOGY ROADMAP FOR THE NEXT-GENERATION CLOUD-EDGE

Prepared by the following members of the Cloud - Edge Working Group



## MAIN CONTRIBUTORS

Manuela Bargis (Telecom Italia), Kjell Bengtsson (Jotne), René Brinkhege (Fraunhofer ISST), Thierry Caminet (Atos), Alfonso Carrillo-Aspiazu (OpenNebula Systems), Marta Casassa (Noovle), Renzo Cavalli (Retelit), Raja Chiky (OUTSCALE), Raphaël Daniel (OVHcloud), Jean-Philippe Defrance (Capgemini), Peter Evans (Atos), Bjoern Fanta (Fabasoft), Stéfane Fermigier (Abilian), Ioannis Fikouras (Ericsson), Andreas Florath (Deutsche Telekom AG), Juan Carlos García (Telefónica), Jörg Heese (IONOS), Brian-Frederik Jahnke (Fraunhofer ISST), Anders Jonson (SecureAppbox), Wenche Karlstad (Tietoevry), Stanisław Krzyżanowski (Cloudferro), Mark Kühner (SAP), Clément Laloux (Amadeus), Nick Law (Atos), Ignacio M. Llorente (OpenNebula Systems), Jean-Pierre Lorré (Linagora), Alberto Marti (OpenNebula Systems), Stefano Negrini (ReLOG3P), Klaus Ottradovetz (Atos), Marzieh Parsa (Noovle), Manuel Lopez Paya (Gigas), Alessandro Percelsi (Telecom Italia), Roberto Querio (Telecom Italia), Christoph Reitenberger (SWD Dormagen), Diego Ricci (Aruba), Dominik Rohrmus (Siemens), Anna Maria Schleimer (Fraunhofer ISST), Sven Schuchardt (Global DMS), Camille Sebire (CapGemini), Luke Skillet (Atos), Enrica Sposato (Noovle), Valentin Steinhauer (Deutsche Telekom),Tomislav Sukser (Deutsche Telekom AG), ), Jérôme Totel (Data4), Arthur van der Wees (Arthur's Legal, Strategies & Systems), Maria Barros Weiss (IONOS), David Vallejo (ARSYS), Giuseppe Villari (Noovle), Paolo Zani (Irideos).

## EDITOR

Dimosthenis Kyriazis (University of Piraeus)

*DISCLAIMER: This document is the second version of the European Industrial Technology Roadmap for the Next-Generation Cloud-Edge. It does not represent an official position of the European Commission, nor the members of the EU Alliance for Industrial Data, Cloud and Edge.*

# ABOUT THE ALLIANCE & THE WORKING GROUP

The **European Alliance for Industrial Data, Edge and Cloud** [1] builds on the European Data Strategy [2] since February 2020. Its creation was endorsed by the European Council conclusions in October 2020 and the Declaration on European Cloud [3], signed by all Member States in October 2020 and announced in the updated European Industrial Strategy [4] in May 2021. The Alliance was launched in July 2021 [5] and started in December 2021 [6]. The Alliance brings together businesses, Member States' representatives and relevant experts to jointly define strategic investment roadmaps enabling the next generation of highly secure, distributed, interoperable, and resource-efficient computing technologies. In addition, the Alliance serves as a platform for exchange on issues of cloud governance, e.g. relating to the public procurement of cloud services. The work is facilitated by the European Commission's Directorate-General for Communications Networks, Content and Technology (DG CNECT).

The **Cloud - Edge Working Group** (WG) brings together the main European Industry players in cloud computing that contributed to the preparation of the current roadmap, and puts effort in identifying investments for the joint development and deployment of the next generation of EU cloud and edge technologies that meet the needs of European businesses. The members of the WG that have co-authored this roadmap are the following:

| | | |
|---|---|---|
| Abilian SAS | Fraunhofer Institute for Software and Systems Engineering ISST | OVHcloud |
| AMADEUS IT | German Edge Cloud | ReLOG3P |
| ARSYS | Gigas | Retelit |
| Arthur's Legal, Strategies and Systems | Global DMS | SAP |
| Aruba SpA | Green Cloud AI | SecureAppbox |
| Atos | IONOS | Siemens |
| Bit4id | Irideos SpA | Sopra Steria |
| Capgemini | Jotne | SWD Dormagen |
| Clever Cloud | Leaseweb | Telefonica |
| CloudFerro | LINAGORA | Tietoevry |
| Data4 | Nokia | TIM SpA – Noovle |
| Deutsche Telekom | OpenNebula Systems SL | TIM SpA |
| Ericsson AB | Orange | |
| Fabasoft | 3DS Outscale | |

The WG is chaired by Ignacio M. Llorente (OpenNebula Systems), co-chaired by Jean-Philippe Defrance (Capgemini) and Mark Kuehner (SAP), and facilitated by Ana Juan Ferrer (European Commission).

# EXECUTIVE SUMMARY

The **European Industrial Technology Roadmap for the Next-Generation Cloud-Edge** provides a collective view of the technology domains and related dimensions requiring strategic investment to enable the joint development and deployment of competitive, secure, trusted, and climate-neutral cloud and edge services across Europe to build the next-generation cloud-edge continuum. Furthermore, this document provides an up-to-date description of major European initiatives, associations, standards, and open source projects for edge and cloud. It also includes an analysis of the opportunities and challenges of digital sovereignty.

The roadmap delivers the main priorities in transversal domains, technology foundations, and sector-specific services driven by relevant use cases and enablers, tackling two cases of priorities:

- Technology Priorities with activities for the specification, research, development, and innovation of the next-generation cloud-edge continuum capabilities.
- Deployment Priorities with activities for the coordination and deployment of cloud-to-edge infrastructure and services to enable the initial roll-out of next-generation use cases on a European-wide scale.

The technology and deployment priorities can be grouped in three main domains:

Becoming the leader in the transversal technology domains that will shape the European cloud and edge offerings on the global market. The future cloud-edge continuum will require new innovative cross-layer and cross-domain services and technologies for carbon neutrality, cybersecurity, trustworthy data exchange, portability, and interoperability that will shape worldwide standards.

Renewing and expanding infrastructure foundations across Europe. The deployment of the cloud-edge continuum requires an increased density of edge and cloud computing facilities backed by ubiquitous connectivity and local 5G networks to deliver the right performance in terms of bandwidth and latency, and managed with advanced orchestration technologies to guarantee efficient infrastructure utilisation.

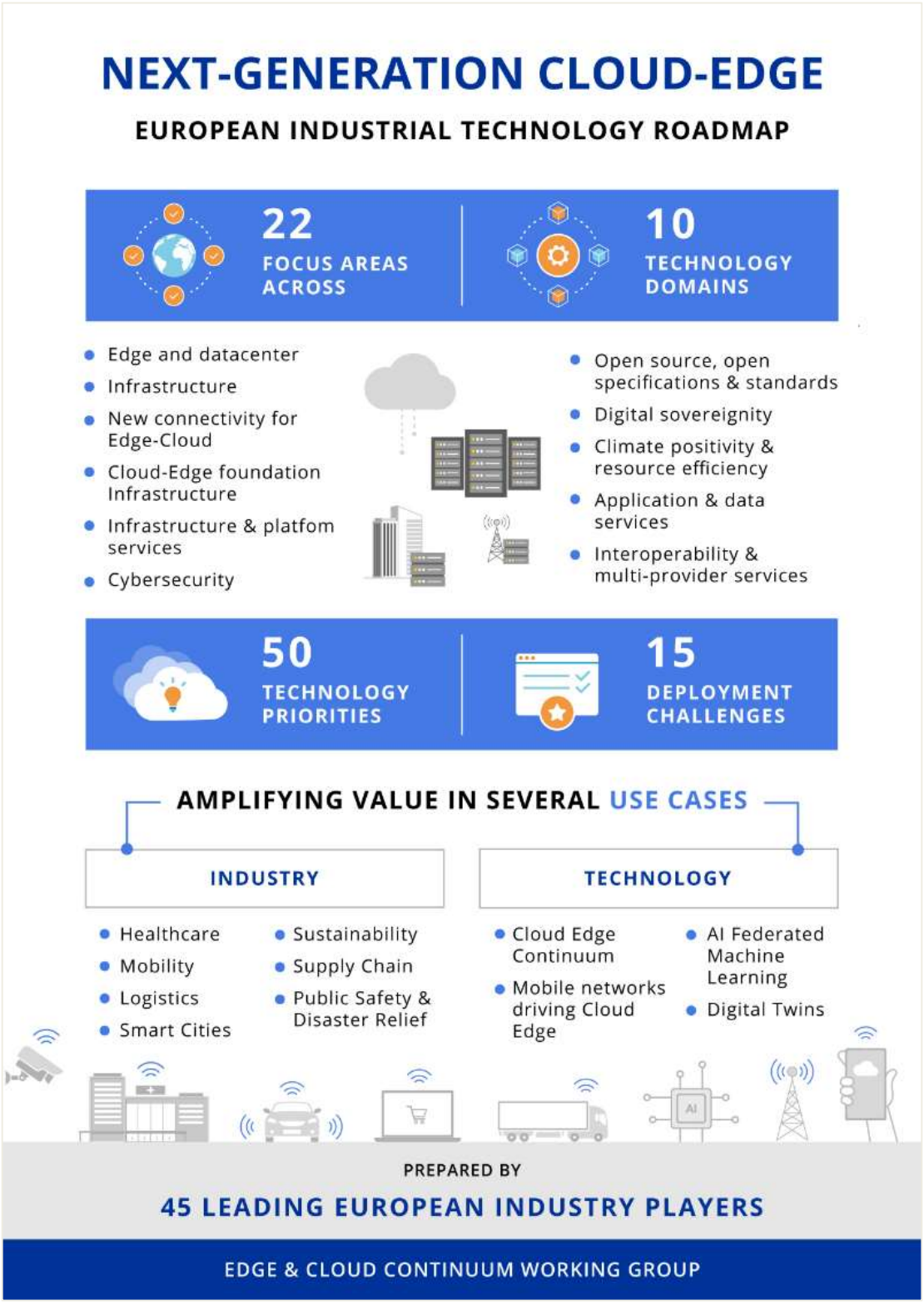
Enabling sovereign and sector-specific services to end users. Existing infrastructure and platform cloud service offerings must be strengthened, with a focus on providing businesses with open source sovereign software solutions for telecommunications, edge, HPC, and quantum computing services; and an open ecosystem of data services and advanced applications.

Although the roadmap contains a high number of important technology and deployment priorities, some of them are especially critical to deliver a solution for the edge-to-cloud continuum in Europe that ensures:

- Competitiveness: that is, a low Total Cost of Ownership (TCO), a solution that is convenient and easy to use. Priorities like orchestration and automation will be of the essence to achieve it.
- Digital sovereignty: certain control over the technological solution, guaranteeing its maintenance and evolution. Priorities like open source code development or federation mechanisms will allow for the delivery of a solution based on key European technological components by European service providers, federated to provide a pan-European, and in the future global, service.
- Kick-start mechanism: to ensure scale is achieved fast to be able to play a role in the global landscape, the engagement of critical sectors like Public Services or Telecom Services at the early stages will be essential. Other more fragmented sectors, like the Industrial sector, will benefit from this kick-start and bring the scale to consolidate the solution.

As a result, a subset of the priorities in this document are considered not only important but essential. These have emerged following a survey that has been conducted among all contributors and participating organizations. The survey has been completed 21 organisations and the results – depicted in the figure, highlight the essential priorities, summing to 45% of the total votes (i.e. all other 60 priorities collectively have received 55% of the votes). These essential priorities are listed below in the order based on the survey voting with the most essential one listed first: (i) Representation in Open Standards and Relation to Norms and Standards, (ii) Open Specifications and Open Source Reference Implementations, (iii) Multi-provider Edge Cloud Federation, (iv) Support Distributed & Interoperable Architectures, (v) Make & Implement EU Regulations Fit for a Digital Sovereign Europe, (vi) Organise EU Standards on Pre-procurement of EU Products, Systems & Services, and (vii) Data-Sharing Business Models.

# TABLE OF CONTENTS


NEXT-GENERATION CLOUD-EDGE
EUROPEAN INDUSTRIAL TECHNOLOGY ROADMAP
22
FOCUS AREAS ACROSS
10
TECHNOLOGY DOMAINS
Edge and datacenter
Infrastructure
New connectivity for Edge-Cloud
Cloud-Edge foundation Infrastructure
Infrastructure & platfom services
Cybersecurity
Open source, open specifications & standards
Digital sovereignity
Climate positivity & resource efficiency
Application & data services
Interoperability & multi-provider services
50
TECHNOLOGY PRIORITIES
15
DEPLOYMENT CHALLENGES
AMPLIFYING VALUE IN SEVERAL USE CASES
INDUSTRY
Healthcare
Mobility
Logistics
Smart Cities
Sustainability
Supply Chain
Public Safety & Disaster Relief
TECHNOLOGY
Cloud Edge Continuum
Mobile networks driving Cloud Edge
AI Federated Machine Learning
Digital Twins
AI
PREPARED BY
45 LEADING EUROPEAN INDUSTRY PLAYERS
EDGE & CLOUD CONTINUUM WORKING GROUP

# INTRODUCTION

Cloud and edge computing are key enabling technologies of strategic importance to achieve the digital transformation of businesses and the public sector in Europe. These technologies provide the data processing capabilities required to enable data-driven innovation and the deployment of common European data spaces in key public and private sectors, as emphasised in the New Industrial Strategy for Europe [7] and the European Data Strategy [2] . From cost savings and faster time-to-market to ground-breaking AI-based data and Industrial Internet of Things (IIoT) services across industry value chains, cloud and edge computing represent tremendous economic potential for citizens, businesses, and public administrations. Europe is no stranger to these technologies. In 2012, the European Commission unveiled its first Cloud Computing Strategy [8], and in October 2020, the 27 EU Member States signed the Joint Declaration on Next-Generation Cloud [9] after reaching an agreement to work together towards deploying resilient and competitive cloud infrastructure and services across Europe.

Even nowadays, the European cloud market struggles to match demand and provide a reliable alternative to global competition. It currently displays a fragmented offering of solutions that are independently innovative but which still do not fully meet users' practical needs in terms of end-to-end coverage and scalability. Both are hard requirements for the massive transformations that are expected to place cloud and edge computing at the core of European business strategies and operations. According to a recent analysis [10], the European cloud infrastructure services sector, which was worth €10.4bn during the second quarter of 2022, has grown tremendously over the past five years and is now five times as big as it was back in 2017. However, the collective market share of the European players has shrunk from 27% to a mere 13%, with the global public cloud infrastructure market converging very rapidly around three large non-European corporations. According to Eurostats' data [11], 41% of the enterprises in the EU use the cloud, with 73% of them being highly dependent on cloud computing. This represents a strong dependency among EU corporate users on non-EU providers, something that raises serious concerns related to personal data protection, sovereignty, cybersecurity, sustainability, external dependencies in strategic sectors or applicable legislation. Europe needs to revert these trends.

The way in which data is stored and processed is gradually changing as the paradigm shift from centralised cloud and data centres to highly distributed edge infrastructures gains momentum. Europe has a unique market opportunity in the next five years to strengthen its data processing technologies by capitalising on the changes to come, particularly those related to edge computing and distributed systems. As highlighted in the European Data Strategy [2], the volume of generated data is increasing very rapidly and a growing percentage of that data is actually being processed at the edge. By 2025, 80% of all generated data is expected to be processed at the edge [2]. Keeping that in mind, it comes as no surprise that Europe's Digital Compass [12] included a target for the deployment of 10,000 climate-neutral, highly secure edge nodes across the EU by 2030. These new

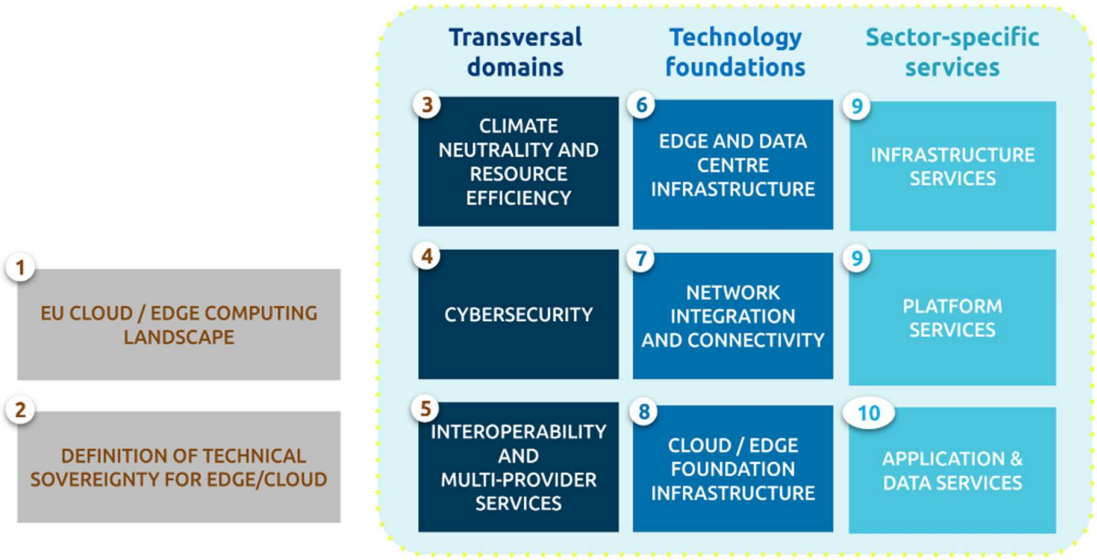
nodes are expected to be distributed in a way that guarantees access to services with low latency wherever businesses are located.

Needless to say, cloud and edge will continue to co-exist, and the integration of these different data processing capacities with more local computing resources will form a computing continuum. The main technology challenge at that point is to ensure supply meets heightened user demands not only in terms of openness, security, privacy, and resilience, but also in terms of energy and resource-efficiency, to finally leverage the edge-to-cloud continuum to address sector-specific requirements. Europe needs to strengthen its own cloud infrastructure and capacities while leading next-generation innovations, focusing its energy on driving advances in technology and competitiveness. It needs to lead the development of multi-cloud and federation technologies leveraging open source and open standards to address the trend towards increasing distribution and decentralisation of data processing and the need to enable federated and vendor-agnostic cloud ecosystems.

As Commissioner Thierry Breton has stated: "in the digital decade, Open Source will be a key element to achieve Europe's resilience and digital sovereignty" [13]. It helps to reduce the market entry barriers and improve cost, increase market competition and technology neutrality. According to the Open Source Software Strategy 2020-2023 [155] and the 2021 study on the impact of open source on the EU economy [14], open source can devise an approach to cloud computing that balances its advantages and risks. It minimises vendor lock-in and gives Europe a chance to create and maintain its own, independent digital approach and to stay in control of its processes, information, and technology, fostering an open ecosystem around sustainable joint innovation. Following the approach defined by the new Standardisation Strategy [15] presented by the European Commission in early February 2022, the new developments should make use of and produce open source implementations of open standards.

As the backbone of the current and future digital economy, cloud and edge computing together with connectivity are also set to play an important role in realising the EU's collective ambition to reduce greenhouse gas emissions by 55% by 2030 [59] and to achieve climate neutrality. Edge and cloud computing are crucial contributors to the common European sustainability goals of the European Green Deal [16], enabling the transformation of different economic sectors of the European economy while becoming more climate neutral and sustainable themselves. While cloud computing facilitates energy efficiency, deployments "at the edge" bring additional benefits, contributing to reducing data traffic and its associated carbon footprint. Given the current geopolitical context and the amount of data that is expected to be generated and processed in the near future, the market will have to start looking as soon as possible for energy-efficient cloud infrastructures and services.

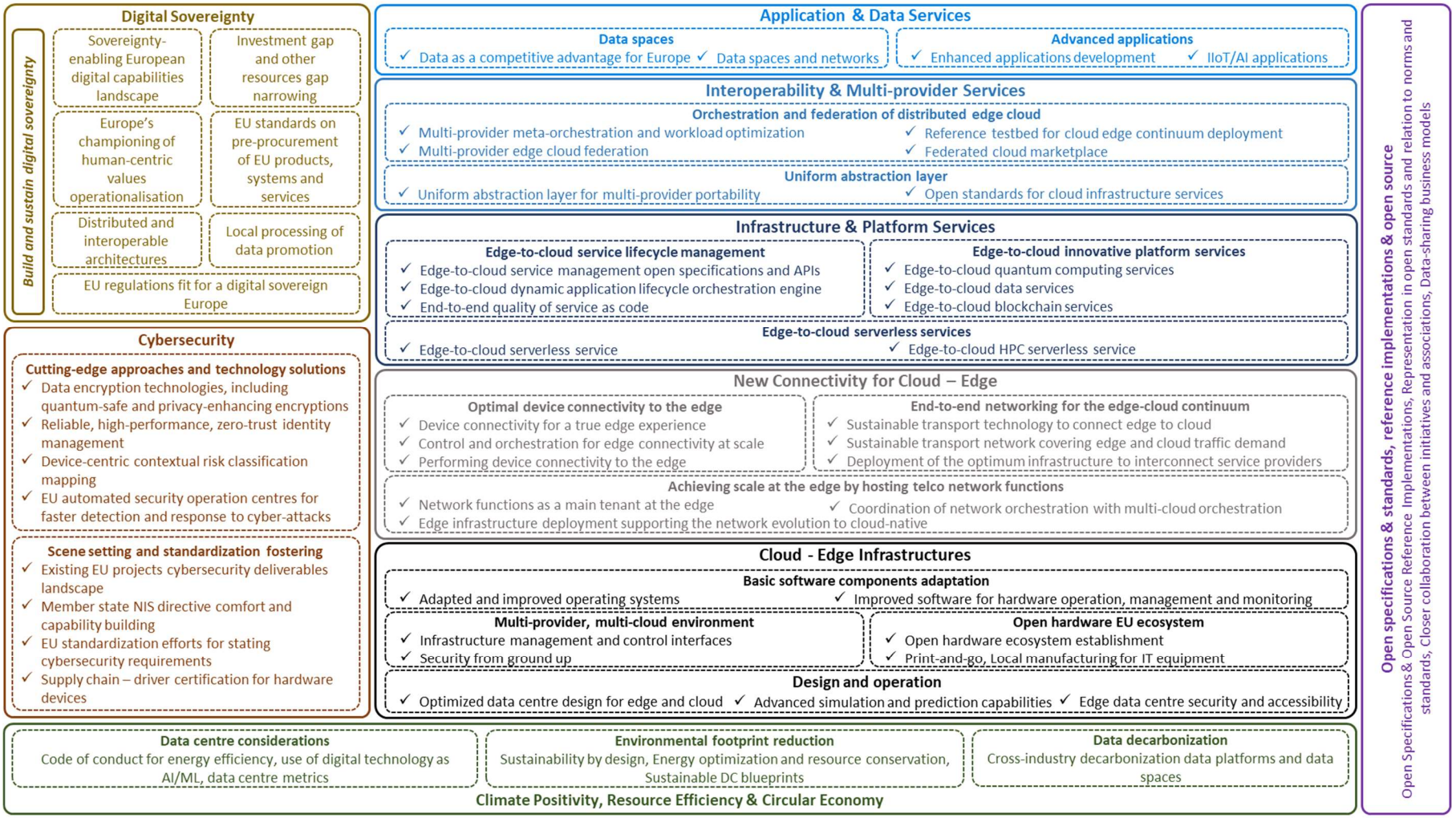
## Roadmap Structure




The structure of the document resembles the structure of the Cloud and Edge Working Group, in which there are two general Task Forces working on the EU edge and cloud landscape and the digital sovereignty respectively, three Task Forces working on energy efficiency, (cyber)security, and interoperability transversal domains, three Task Forces working on the computing and networking infrastructure technology foundations, and two Task Forces working on infrastructure and platform sector-specific services. This document also includes a final section (Section 11) that summarises the main *challenges of the deployment of the cloud-edge continuum* in the European market.

Per priority the main key drivers are summarized, the representative use cases (following the use cases cited in this roadmap) that would benefit from the proposed recommendations, the dependencies – as requirements for the realisation of the priority, and the actual recommendations. These are presented in a temporal categorization (i.e. short, mid and long term). Furthermore, priorities in each section of this roadmap are grouped based on their contents in the respective Focus Areas.

The following figure presents the main technology and deployment priorities as identified by each Task Force, grouped under the corresponding Focus Areas.


Digital Sovereignty
Build and sustain digital sovereignty
Sovereignty-enabling European digital capabilities landscape
Investment gap and other resources gap narrowing
Europe's championing of human-centric values operationalisation
EU standards on pre-procurement of EU products, systems and services
Distributed and interoperable architectures
Local processing of data promotion
EU regulations fit for a digital sovereign Europe
Cybersecurity
Cutting-edge approaches and technology solutions
✓ Data encryption technologies, including quantum-safe and privacy-enhancing encryptions
✓ Reliable, high-performance, zero-trust identity management
✓ Device-centric contextual risk classification mapping
✓ EU automated security operation centres for faster detection and response to cyber-attacks
Scene setting and standardization fostering
✓ Existing EU projects cybersecurity deliverables landscape
✓ Member state NIS directive comfort and capability building
✓ EU standardization efforts for stating cybersecurity requirements
✓ Supply chain – driver certification for hardware devices
Application & Data Services
Data spaces
✓ Data as a competitive advantage for Europe ✓ Data spaces and networks
Advanced applications
✓ Enhanced applications development ✓ IIoT/AI applications
Interoperability & Multi-provider Services
Orchestration and federation of distributed edge cloud
✓ Multi-provider meta-orchestration and workload optimization
✓ Multi-provider edge cloud federation
✓ Reference testbed for cloud edge continuum deployment
✓ Federated cloud marketplace
Uniform abstraction layer
✓ Uniform abstraction layer for multi-provider portability
✓ Open standards for cloud infrastructure services
Infrastructure & Platform Services
Edge-to-cloud service lifecycle management
✓ Edge-to-cloud service management open specifications and APIs
✓ Edge-to-cloud dynamic application lifecycle orchestration engine
✓ End-to-end quality of service as code
Edge-to-cloud innovative platform services
✓ Edge-to-cloud quantum computing services
✓ Edge-to-cloud data services
✓ Edge-to-cloud blockchain services
Edge-to-cloud serverless services
✓ Edge-to-cloud serverless service
✓ Edge-to-cloud HPC serverless service
New Connectivity for Cloud – Edge
Optimal device connectivity to the edge
✓ Device connectivity for a true edge experience
✓ Control and orchestration for edge connectivity at scale
✓ Performing device connectivity to the edge
End-to-end networking for the edge-cloud continuum
✓ Sustainable transport technology to connect edge to cloud
✓ Sustainable transport network covering edge and cloud traffic demand
✓ Deployment of the optimum infrastructure to interconnect service providers
Achieving scale at the edge by hosting telco network functions
✓ Network functions as a main tenant at the edge
✓ Edge infrastructure deployment supporting the network evolution to cloud-native
✓ Coordination of network orchestration with multi-cloud orchestration
Cloud - Edge Infrastructures
Basic software components adaptation
✓ Adapted and improved operating systems
✓ Improved software for hardware operation, management and monitoring
Multi-provider, multi-cloud environment
✓ Infrastructure management and control interfaces
✓ Security from ground up
Open hardware EU ecosystem
✓ Open hardware ecosystem establishment
✓ Print-and-go, Local manufacturing for IT equipment
Design and operation
✓ Optimized data centre design for edge and cloud ✓ Advanced simulation and prediction capabilities ✓ Edge data centre security and accessibility
Data centre considerations
Code of conduct for energy efficiency, use of digital technology as AI/ML, data centre metrics
Environmental footprint reduction
Sustainability by design, Energy optimization and resource conservation, Sustainable DC blueprints
Data decarbonization
Cross-industry decarbonization data platforms and data spaces
Climate Positivity, Resource Efficiency & Circular Economy
Open specifications & standards, reference implementations & open source
Open Specifications & Open Source Reference Implementations, Representation in open standards and relation to norms and standards, Closer collaboration between initiatives and associations, Data-sharing business models

# USE CASES AND ENABLERS

The technology and deployment priorities defined in this roadmap are driven by emerging, highly innovative use cases and enablers that are critical for strengthening the position of the EU industry regarding next-generation cloud and edge technologies, and industrial data. This a list set forth below some highlights of the many industry and technology use cases considered in this roadmap.

## Industry Use Cases

### Healthcare: "Next-Gen Engagement" & Human Centricity

The healthcare sector is shifting towards tele-health and personalised medicine. This requires cross-vendor interoperability and standardised data sharing. The scenarios like remote surgery require high resilience and low latency edge-cloud solutions.

### Mobility: Smart & Secure Mobility

Urban growth requires a shift of the mobility / transport system towards optimised energy and resource consumption and usability. Mobility-as-a-service and autonomous driving solutions require real time exchange data between devices and scalable capacity to run AI models in the cloud.

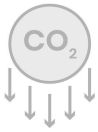
### Logistics: Global Freight & People Logistics

Global Logistics is a backbone of industry supply chains. It shifts towards digitisation for increased efficiency, effectiveness, and sustainability, while reducing impact on energy consumption and distribution cost. Its goals are the accelerating of zero-emission freight transport and the setup of fast and reliable logistics information systems based on an edge-cloud architecture.

### Public: Smart Cities

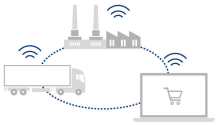
Smart city services optimise resource usage and improve the quality of life by connecting and utilising data from different sectors (e.g. power plant, utilities, infrastructure, health, mobility, etc.). As data processing is the enabler for smart cities, the edge to cloud infrastructure is a key/critical success factor to provide the right data at the right time and to ensure data/digital sovereignty.

### Sustainability: Cross-Industry Data Decarbonisation Platforms




Improve the visibility and control of the greenhouse gas (GHG) emissions. Data platforms and data spaces provide multiple industries with new services to reduce their emissions in line with increasing societal and regulatory requirements. The combination of financial, performance, and emissions data is important, ensuring appropriate privacy and security.

### Supply Chain: Digital Supply Chain



The digital supply chain is a smart, value-driven, efficient process to generate new forms of revenue and business value for organisations and to leverage new approaches with edge-cloud technologies. It is about transparency and control of virtual and physical goods and services.

### Public: Public Safety & Disaster Relief

Public safety critical services (e.g. police, fire and rescue, medical emergency) deal with incidents in the most effective and efficient way, especially when larger events occur. Leveraging on a large-scale public and interoperable safety platform will enable these services to produce common and standard reaction plans to events, achieve faster data exchange among local services across the EU region, and ultimately simplify coordination and cooperation among services.

## Technology Use Cases (Enablers)

### Infrastructure: Edge-to-Cloud Continuum

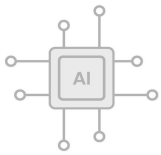
The edge-to-cloud continuum brings several new complex challenges compared to standard distributed computing systems because of the heterogeneous computing environment, heterogeneous and dynamic network environment, node mobility, and limited power capacity.

### Telecommunications: Mobile Networks Driving Cloud Edge

Telecommunication applications (network Functions from access, transport and core networks) require a very distributed computing infrastructure as many of these functions need to be executed close to the user, such as the units that process the baseband signal of mobile radio stations. On the other hand, some network functions have specific requirements in terms of time synchronization and signalling that demand specific hardware configurations (acceleration) and some adaptations of the cloud stack. Finally, the complex

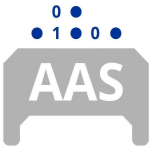
mesh of interrelationships between network components requires high levels of orchestration and automation for network deployment and management.

### Applications: AI Federated Machine Learning




One of the main concepts in the computing continuum is the use of caching to bring the intelligence closer to the edge, instead of leaving the intelligence centralised in cloud servers. Federated learning at the edge trains AI models across edge nodes without the need to transfer data to the cloud to preserve privacy and bandwidth.

### Digital Twins: Linking Operational Technologies (OT) Systems to IT Representation




A prerequisite for the listed use cases is the capability to make data from physical devices (e.g. factories, machines, cars, medical operation rooms) available to an IT system which is able to process and analyse the data and drive actions back to the physical world (closed loop). This requires controlled resilience, latency, scalability, in a controlled, secure framework.

# SECTION 1: EUROPEAN CLOUD AND EDGE LANDSCAPE

The edge computing paradigm is the logical evolution of the cloud computing model, minimising the transfer of data across the network to centralised infrastructures, supporting distribution of workloads and thereby, supporting amongst others resilience and real-time operations, while at the same time reducing energy consumption and the carbon footprint. Therefore, this implies balancing centralised computing facilities with computing at the edge. Hence, a continuum from edge to cloud is the next technological step to enable and grow data-based digital use cases and business models. The decrease in the market share of European cloud providers as shown in Figure 1 (3 percentual points decrease since the May 2021 report) can be mitigated by an increase of cloud-edge capacities and capabilities driven by data being generated at the edge. The need for a edge-to-cloud continuum creates a unique opportunity to increase Europe's cloud capabilities and will provide a sovereign foundation for new digital business models.

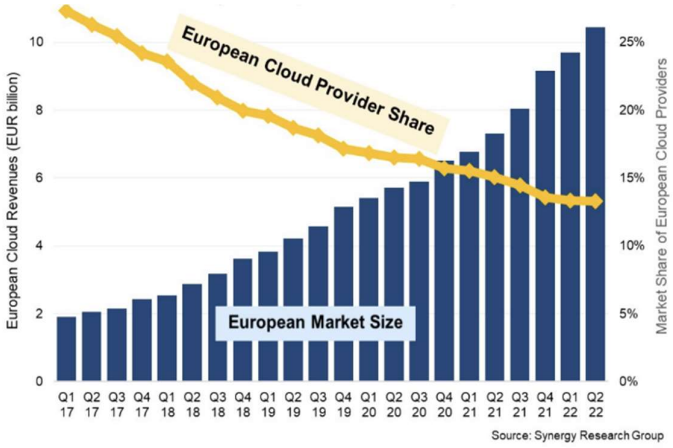



*Figure 1: European Cloud Provider Share of Local Market*

This section assesses the main edge and cloud undertakings that have emerged in Europe (including those with a global scope), the key international standards and open source ecosystems, and the business model challenges, and gives an overview of the investment and funding opportunities.

The European cloud and edge landscape is embedded in EU Initiatives to strengthen Europe's digitalisation and to build on European knowledge and attitudes. Specific European industry topics like Industry 4.0 initiate major projects like Catena-X [18] and Manufacturing-X [19] or Smart Connected Supplier Network (SCSN) [20] and EONA-X [21] with the goal of sharing data between different providers by creating data spaces. European Alliances collaborate with these projects on various topics like AI, data spaces, and infrastructure to feedback findings from their working groups to the market players. The market push for the data spaces creation is supported by Important Projects of Common European Interest (IPCEI) [26]. A special focus of the EU lies on the

upcoming IPCEI on Next-Generation Cloud Infrastructure and Services (IPCEI-CIS). Important for their success is a fast go-live of solutions and a spill-over effect to exemplary SMEs across Europe. In this context, Figure 2 shows major European initiatives, associations, and projects for edge and cloud, both with public and/or private investments. They are clustered in several main areas like infrastructure, data spaces, and services. Managing and aligning these initiatives across Europe to foster technological developments and their dissemination is an important task for the future.

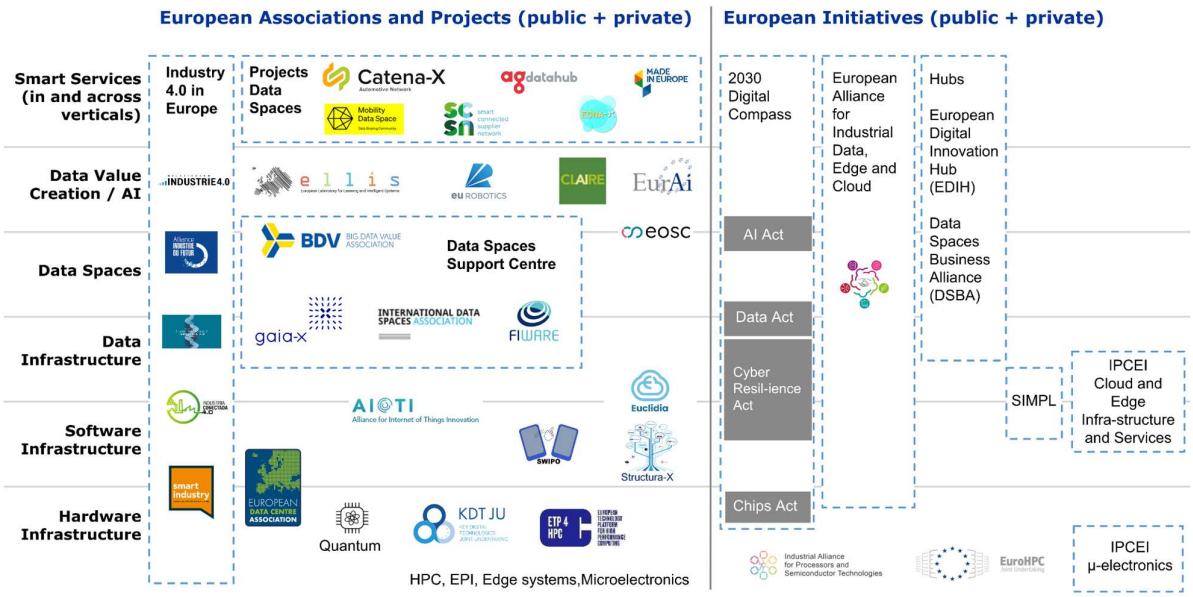



*Figure 2: European associations, projects, and initiatives*

Use cases are an important driver for the presented recommendations of the Alliance. Examples are Industry 4.0 use cases across Europe or vertical focused projects like Catena-X [18] for the automotive sector. The European AI, data spaces, and infrastructure associations work jointly in the Data Spaces Support Centre (DSSC) [27] project to create the building blocks for the technology- and business- related topics.

The Hubs are provided and operated by several organisations and partially funded by the EU. Hubs are important since they operate close to the local markets and provide first-hand experience and the necessary use cases.

The IPCEI on Next-Generation Cloud Infrastructure and Services (IPCEI-CIS) aims to create innovations that work on the computing continuum from edge to cloud and are therefore very important for the work of the Alliance.

Further information on the organisations shown in Figure 2 are summarised in Table 1 covering from a high-level perspective their membership configuration, their EU relation, and their funding situation. The membership ranges from industry and / or governments and / or Research and Technology Organisations (RTOs) to national associations. However, the membership may be restricted to EU-headquartered organisations and international members may be limited in their membership functions. Their funding is usually based on membership fees but also covers the provisioning of funding for certain activities like projects, events, or the expectation of funding from various sources like governments:

| Name | Area | Hub structure | Membership | EU only | Funding (provided / expected) |
|---|---|---|---|---|---|
| **Catena-X [18]** | Automotive, Supply Chain | Yes (DE & FR) | Industry, RTO | No | Yes / Yes |
| **EONA-X [21]** | Mobility, Transport, Tourism | No | Industry | No | No / Yes |
| **Big Data Value Association (BDVA) [22]** | Big Data, AI | EU | Industry, RTO | No | Yes / Yes |
| **European Open Science Cloud (EOSC) [23]** | Scientific Research | No | RTO | Yes | Yes / Yes |
| **Gaia-X [24]** | Federated Data Infrastructure | Global | Industry, Gov, RTO | No | No / No |
| **Alliance IoT (AIOTI) [25]** | IoT | No | Industry, RTO | No | No / No |
| **IPCEI-CIS [26]** | Edge, Cloud | No | Industry, Gov, RTO | Yes | Yes / N/A |
| **Data Spaces Support Centre [27]** | Data Spaces | No | Industry, RTO | Yes | Yes / No |
| **European Data Centre Association (EUdata centreA) [28]** | Cloud | No | Industry | No | No / No |
| **EUCLIDIA [29]** | Cloud | No | Industry | Yes | No / No |

*Table 1: Information on European associations, projects, and initiatives*

# Focus area: Open specifications and standards, reference implementations, and open source

The European cloud and edge landscape along the entire industry value chain is using a broad range of normative, standardisation, and de-facto standardisation rulings, as well as a number of open source technologies. Figure 3 provides a selected overview of some relevant main standardisation activities and open standards and open source initiatives in Europe, some of them operating globally too:

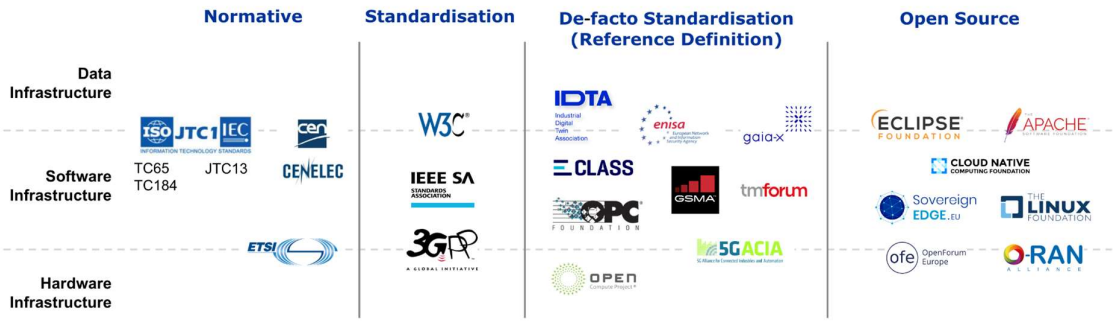



*Figure 3: Main standardisation activities, reference definition initiatives, and open source communities in Europe*

A broad range of norms and (de-jure and de-facto) standards exist in Europe and worldwide. In such activities open standards and open source technologies are gaining increasing importance in the last decades, which is why they cover the main part of the technology priorities in the following paragraphs. Various standardisation and standard-setting organisations are active in many technological fields of edge and cloud: trust and cybersecurity, management of data and networks, deployment of software and data as well as the necessary enabling technologies. Europe may foster its standardisation, with the intention from the beginning of reaching a global scale. Open source communities are increasingly engaged in creating reference implementations that are synchronised with standardisation activities. To this end, the fully synchronised relationship between the definition of open standards and the production of open source implementations is crucial. Moreover, the (on average) slower pace of the formal standardisation and normative processes asks for de-facto standard approaches. These are delivered by industry-led organisations that are usually non-for-profit associations. This should be better synchronized with the necessary normative activities in Europe since norms are of great importance for major industries in Europe.

## 1.1. Technology Priority: Representation in Open Standards, Relation to Norms & Standards, Industrial Data

### Key drivers

The various standardisation and normative activities for industrial edge and cloud are operated by European norming organisations like CEN, CENELEC, and ETSI, and international bodies like IEC (TC65) and ISO (TC184/SC4). As these operate traditionally with the OT (Operational Technologies) industry, the IT industry usually operates on standards maintained by major global organisations like IEEE Standards Association (SA), the World Wide Web Consortium (W3C) or the 3rd Generation Partnership Project (3GPP).

Relatively newer are standard setting organisations like the Industrial Digital Twin Association (IDTA) [30], ECLASS [31] or the OPC Foundation [32] which focus on information modelling and interoperability for industry. The convergence of OT and IT is one focus of the work of these standardisation and normative organisation since the beginning of Industry 4.0. Due to the heterogeneous situations of OT and IT applications for instance in terms of the application life-cycles (OT: long, IT: short) the convergence is a slow market adoption process. Nevertheless, the major technical areas are jointly addressed by these organisations. Examples of these areas are architectural foundations including the terminology and software classifications (e.g. firmware, services, applications), supporting technologies (e.g. virtualisation, containers, serverless computing, microservices), networking including virtual networks, data and its definitions, management and deployment of software, cybersecurity and privacy, latency and real time, mobile computing and mobile/IIoT devices.

The GSM Association (GSMA) [154] is an industry organisation of mobile network operators supporting standardisation initiatives like the CAMARA Telco Global API Alliance [107] and business initiatives like the Open Gateway agreement [33]. The TM Forum [34] is a global industry association for service providers and their suppliers in the telecommunication industry fostering the development of open APIs. The 5G Alliance for Connected Industries and Automation (5G ACIA) [35] fosters the adoption of wireless technologies in the OT sector running open source projects. The Open Compute Project (OCP) [36] fosters the adoption of open innovations for cloud and edge technologies at use in in data centres.

The definition of *Industrial Data* is according to ISO TC 184/SC 4 the following: "Standardization of the content, meaning, structure, representation and quality management of the information required to define an engineered product and its characteristics at any required level of detail at any part of its lifecycle from conception through disposal, together with the interfaces required to deliver and collect the information necessary to support any business or technical process or service related to that engineered product during its lifecycle."

EU Reports, in the Code of Practice on standardisation in the European Research Area [37] STANDARDS - offer a basis for the integration of diverse technologies into complex, innovative

systems and solutions, and enable interoperability between components, products and services thereby avoiding vendor lock-in and providing more choice for customers globally – a critical role in a world undergoing digital transformation across all industries and sectors.

Today's manufacturing industries are under continuous pressure to deliver competitive products faster. At the same time, they must reduce the development cost and the cost of product ownership. In addition, they must protect their intellectual property while working in shared environments and while sustaining business growth and competitiveness. To achieve this goal, collaboration across the product development lifecycle is critical. Unfortunately, collaboration introduces many complications that must be addressed to ensure the integrity and consistency of product development information. These product development processes now also span increasingly complex business environments that bring together multiple companies, each with their own systems and processes. This challenge of global communication of product data across systems and processes of industrial stakeholders can only be solved by a common understanding of the shared data. It is not sufficient to share distinct documents; the need is to agree how to describe each and all aspects of products. The scope of the shared information we call "Industrial Data". Industrial Data are sets of structured, machine interpretable product data.

A data set may describe product geometry, a bill of material or a maintenance schedule. To solve the industrial challenge of digitalisation, it must be possible to merge such individual data sets into product descriptions of growing completeness. They will enable Digital Twins.

Data sets are machine interpretable when they follow the rules of a data model. Global communication requires an agreed data model for industrial data to be publicly available; vendor-specific proprietary specifications do not provide data ownership and flexibility of implementation.

The ISO 10303 standards, STEP, that support CAD/PLM/FEM/SIMULATION, IoT, Manufacturing, Circularity and Logistics, address these requirements. They have been developed in a close collaboration between industrial end users and software vendors. A great share of the current ISO 10303 data model is implemented in commercial off-the-shelf engineering applications. Hence complex industrial solutions will have a life cycle of 50-100 years, and what IT systems will be used in 20 years from now will not be able to envision. As for Industrial Data, ISO 10303 was introduced in 1994, and today manage > 80% of such data exchange, sharing and archiving processes. This is a major achievement over the last 30 years. Besides solving data interoperability, they also open for solutions of Long-Term Archiving and Retrieval (LOTAR) as defined by the AIA/ASD standardization effort of the same name.

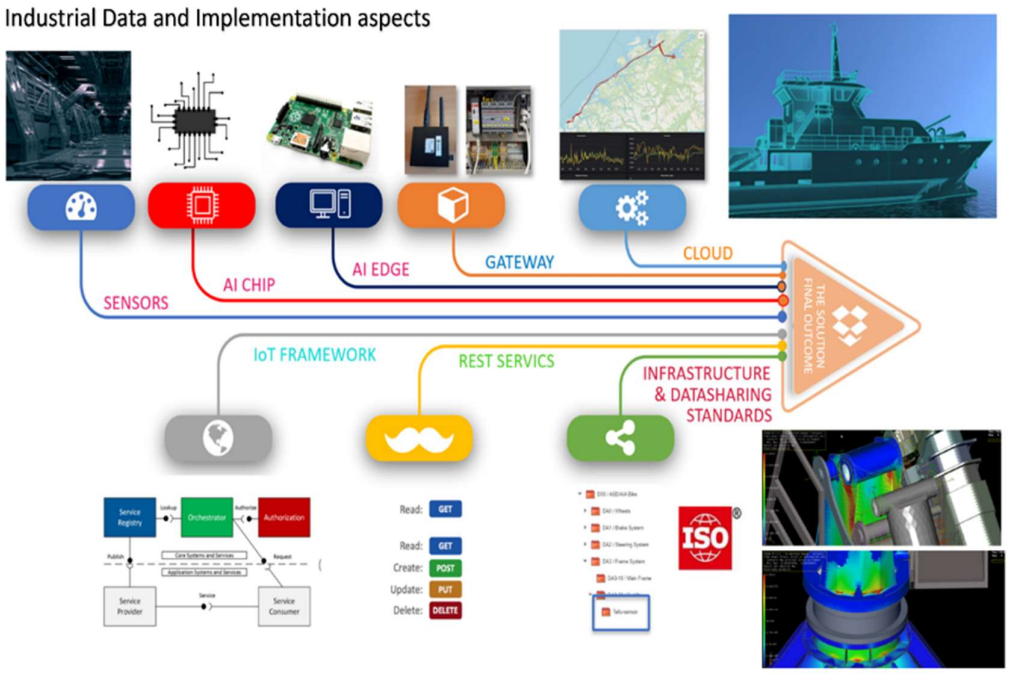



*Figure 4: Challenges for Industrial data and Digital Twin implementations*

In this context, the ISO committee for "Industrial Data", ISO/TC 184/SC 4, specifies standards in the area of industrial data. The mission of SC 4 is to develop and promulgate standards for the representation of scientific, technical and industrial data, to develop methods for assessing conformance to these standards, and to provide technical support to other organizations seeking to deploy such standards in industry. The implementation of the SC 4 standards enables the system platform independent exchange of product related information throughout the product lifecycle. The standards are applicable in computer systems for several purposes such as the exchange, sharing and archiving of product information, the description of products by their properties, the visualization of product and product behaviour, the modelling of product engineering processes, the industrial data quality, etc. Many standards developed within SC 4 are multiple part standards, which cover data model definition, reference data, implementation approaches, data quality management and conformity testing to meet a broad range of industrial business scenarios. The scope of SC 4 includes all the industrial data related to products including, but not limited to geometric design data and tolerance data, material and functional specifications, product differentiation and configuration, process data, project data, production data, lifecycle data, data and information quality management, etc.

Based on the above, the goal of SC 4 is the creation and maintenance of standards that enable the capture and use of information comprising a computerized product model in a neutral form without loss of completeness and integrity throughout the lifecycle of the product. Specific objectives include among others the flexibility to permit expansion without invalidating existing portions of the standard, the efficiency for processing, communication, and storage, the minimum

possible set of data elements, the separation of data content from physical format, the support for security procedures, and the methods and criteria for the management of data quality. The overall vision is based on a business environment with a network of enterprises, interrelated by producer-purchaser and partnership interactions. At the highest level, the purchaser is the consumer of the product; at intermediate levels, producer and purchaser are part of a supply chain; at the lowest level, the producer is the supplier of raw material. Partnerships are collaborations between enterprises at the same level. The vision is of a data model and terminology that includes the product and process data necessary for the operation of all the enterprises in this network, in a consistent manner. This data model and terminology is easily partitioned, both as to ontology, schema, and to actual data, into subsets representing the data necessary for the successful operation of business functions in each individual enterprise. Such subsets support all the data requirements for the product and process development activities within that enterprise.

### *Recommendations*

| | |
|---|---|
| *Short-term* | European voices and seats in global open standardisation bodies and communities should be strengthened. The representation in open standards committees and communities should become an integral part of European and national funded projects. |
| *Mid-term* | Structured positioning of resources in industry bodies like international standardisation organisations. Standardised legal frameworks that cover all aspects of Intellectual Property (IP), open licenses, data sharing, freedom to operate and competition law. Fostering of standardisation education in general and with a certain focus on open standards specifically (e.g. university, training on the job, etc.). |
| *Long-term* | Open standards and specifications as well as open source technologies and implementations are an important long-term market factor in Europe. It should be ensured that European technologies, innovations, and products are at the core of the industry solutions worldwide. A pre-requisite is the close alignment with industry organisations on a global scale. Further, EU and nations should consider legislation by law and in new contracts to mandate the use of standards for Industrial Data, equivalent as EU did for the USB-C for small and medium-sized portable electronic devices, where buyers can choose whether to purchase new device with or without charging device. Doing so, this will open up and increase the use of industrial data dramatically. |

## 1.2. Technology Priority: Open Specifications & Open Source Reference Implementations

### Key drivers

Open specifications and the corresponding open source reference implementations are attractive for solving the heterogeneous multi-vendor industry market challenges like circular economy, green house gases reporting or digital twins. Combining open specifications with open source can accelerate the market development and enable quick market take-up of innovative cloud-edge solutions. It is an important element to developing a European-wide cloud and edge infrastructure. The interoperability of these Infrastructure-as-a-Service offerings, for example, remains among the challenges being identified by the Alliance (from skills to control/resiliency and even security).

Open source projects and communities for industrial data, edge, and cloud technologies are usually run by not-for-profit entities. Some industry organisations as representative examples are the following: (i) the Linux Foundation [38], a US-based organisation founded in 2000, with a new EU Brussels-based entity established being announced in September 2022: Linux Foundation Europe [39]; especially relevant is LF Edge [40], a niche community focused on edge computing, (ii) the Cloud Native Computing Foundation [41], a Linux Foundation community that was founded in 2015 to help advance container technologies, (iii) the Eclipse Foundation [42], which was created in 2004 as an independent not-for-profit corporation to act as the steward of the Eclipse community, with the Brussels-based international not-for-profit association operating the Edge Native Working Group [43] and also an IoT Working Group [44], (iv) the Apache Software Foundation [45], a US-based organisation established in 1999 that develops, stewards, and incubates more than 350 open source projects and initiatives covering a wide range of technologies, including AI, Big Data, Cloud Computing, DevOps, IoT, and Edge Computing, (v) the Sovereign Edge.EU [46] initiative, launched in 2021 as a community aiming to foster innovation and collaboration between European open source technology providers, contributing to building a cloud/edge ecosystem in Europe and working in joint research and innovation projects focused on edge computing, (vi) OpenForum Europe (OFE) [47], a Brussels-based organisation launched in 2002 to accelerate, broaden, and strengthen the use of Open Source Software (OSS) and open standards in business and government; OFE is supported by major IT vendors, works closely with the European Commission, the European Parliament, national and local governments, (vii) the O-RAN Alliance [48], founded in 2018 as an open technical organisation to re-shape the Radio Access Network (RAN) industry towards more intelligent, open, virtualised and fully interoperable mobile networks, (viii) the OW2 a Europe based association supported by many European large organisations and academia aiming at facilitating the development, deployment and management of distributed applications with a focus on open source middle-ware and related development and management tools, and (ix) the OpenInfra foundation, supporting the development and adoption of open infrastructure globally, across a community of over 110,000 individuals in 187 countries, by hosting open source projects and communities of practice [49].

## Dependencies

*4.8. Deployment Priority: Supply Chain – Driver Certification for* Hardware Devices*:* Define a secure European Open Reference Architecture to promote a Secure-by-Design mindset and offer a foundational Root of Trust architecture.

*5.1. Technology Priority: Open Standards for Cloud Infrastructure* Services*:* Ensure EU is represented and influential in existing standardisation and normative bodies.

*5.2. Technology Priority: Uniform Abstraction Layer for Multi-provider* Portability*:* Follow open standards and open source software where possible to build the abstraction layer.

*5.3. Technology Priority: Multi-provider Meta-Orchestration and Workload* Optimisation*:* Leading European providers with relevant open source software developers to work together in the creation of a community-managed platform capable of solving the key federation challenges in the edge-to-cloud continuum.

*7.2. Technology Priority: Control & Orchestration for Edge Connectivity at* Scale*:* The development of standard and open Network-as-a-Service (NaaS) APIs will provide the means to implement these features more efficiently.

*8.1. Technology Priority: Establish an Open Hardware* Ecosystem*:* Define and standardise open hardware based on existing standards for different use cases through the edge-to-cloud continuum.

*Focus area: Edge-to-Cloud Service Life Cycle Management:* Specify a cloud & edge software stack with standardised and open interfaces, and ultimately ensure their implementation in software offerings.

*9.7. Technology Priority: Edge-to-Cloud Data* Services*:* Build a scalable open source data solution to manage data exchanges between massively distributed and heterogeneous actors over the edge-to-cloud continuum.

*10.1. Technology Priority: Data as a Competitive Advantage for* Europe*:* To build upon the existing EU regulations and open standards to promote data and applications.

*10.2. Technology Priority: Data Spaces and* Networks*:* In order to foster the development of data spaces and networks under the principles of interoperability and fair access to data, it is necessary to manage data as digital commons by promoting openness and data model standardisation. It is important that enterprises and primarily SME and start-ups share their data under their control.

*Focus area: Advanced applications:* Foster the development of an open marketplace for data and cloud that will leverage scalability and network effects by providing an open European application marketplace to facilitate dissemination and exploitation.

### *Recommendations*

| | |
|---|---|
| *Short-term* | Strengthen existing (and create new) open source software communities, led by European organisations, to manage and maintain important technologies in the long term as well as to lead open source reference implementations. Educate organisations on how to generate value with and from open source projects as a driver to join and contribute to open source projects and communities. |
| *Mid-term* | Coordinated promotion of European open source technologies and cloud-edge platforms in education and in other EU strategic sectors. |
| *Long-term* | Active promotion of open source implementations of open standards and specifications, synchronizing and integrating them with the normative and standardisation roadmaps of major organisations and their existing implementations. |

## 1.3. Technology Priority: Closer Collaboration between Initiatives and Associations

#### Key drivers

The adaptation of open source technologies and open standards to the marketplace is fundamentally dependent on a close working relationship between their respective organisations. This cooperation already exists among some organisations and standard bodies. However, it is in most cases not fully operationalised and is particularly lacking in association-driven de facto standardisation. Synergies must be created to achieve the objectives of the initiatives summarised in Figure 2 in a timely, cost-effective, and resource-efficient manner.

The rich landscape of initiatives aiming at a thriving European data economy is a development that underlines the relevance of the initiatives for the industry, the urgency of the challenges, and the willingness to contribute to tackling them in a collaborative way. The industry's participation in the numerous technology initiatives, which is positive in nature, also highlights new organisational requirements and risks as well as losses in effectiveness due to increased coordination and integration efforts. Additionally, there is a significant risk of inefficient resource allocation. As the complex landscape of associations and initiatives has grown considerably, with public funding and a significant contribution of industrial resources, there is also a risk that these valuable resources and knowledge will be lost if efforts are not aligned properly.

In an extreme scenario, the misalignment between the associations and the initiatives would expose them to the following risks: First, compete with each other for industry resources, such as financial (in the form of membership fees) or human (in the form of expertise and time) ones. Second, run the risk of being a burden, rather than a benefit, to the industry through the increasing consumption of valuable resources in multiple initiatives that could be invested directly in business activities. Especially in today's dynamic and fast-moving times, the opportunity costs for industrial companies are high when they decide to contribute resources to non-profit organisations. Participation will decrease in the future if resources are not used effectively to achieve commonly shared goals. This would not only harm individual companies and initiatives but would also hamper the overall effort to create a common, thriving European digital economy, and give a negative impression of European effectiveness and values. From the perspective of the associations and initiatives, uncertainty about, a complex landscape with many interdependencies hampers the efficient work on critically needed content. The management and alignment of different associations has emerged as a resource-consuming issue. There is a constant risk of duplicating work that is redundant or competes with the results of other initiatives. Despite the fact that a certain degree of competition may be fruitful and increase the overall quality, at a technical level, the complexity and heterogeneity on various conceptual levels pose serious challenges to the integration of open source technologies, making them unsuitable for large-scale ecosystem approaches that require seamless and secure integration.

Furthermore, the scenario carries the risk of creating silos for different ecosystems and domains that may not be able to be resolved at a later stage. The aim is a diverse landscape and a broad range of high-quality technologies that reinforce and empower rather than block each other as part of the overall strategic goals of the EU.

### Relevant use cases / application domains

The relevant applications refer to the efficient integration of services, data, and network environment across different providers in general.

Inherently, this concern presents a cross-cutting issue for each of the eleven use cases mentioned in Use Cases and Enablers. The cross-cutting issue refers to the -interoperability of global standards and the inter-domain-compatibility. Technological compatibility across domains is important for scenarios that cover different overarching use cases and might occur in settings such as, for example, the *Cross-Industry Data Decarbonisation Platforms, Supply Chain, Mobility* and *Public Smart Cities*. In particular, use cases that rely on complex and long data chains and service compositions, such as in the application of AI, benefit from interoperability and eased integration demands.

The increased collaboration is relevant also for emerging initiatives in a nascent stage, as well as technologies in a low maturity state and industrial research and development efforts. It is in those early stages that the foundation for a large-scale integration of services is designed.

### *Recommendations*

| | |
|---|---|
| *Short-term* | Strengthen the cooperation of EU open source initiatives and organisations with the existing associations and bodies to closely align and collaborate on open source specifications and standards to enable short-term market update of both industries, i.e. the IT and the OT industries. |
| *Mid-term* | The cooperation and alignment of open source initiatives and EU projects towards the EU roadmaps should be strengthened. Beside formal and top-down efforts to align initiatives and, therefore, their different communities, efforts to foster and incentive a bottom-up alignment of different member communities across initiatives could also be created. |
| *Long-term* | The collaboration of all relevant industry organisations and open source bodies should be well-established and supported by the EU through active collaboration projects and EU support actions. |

## 1.4. Deployment Priority: Data-Sharing Business Models

#### Key drivers

The importance of data and services (smart services) in the value creation forces companies to critically reflect on their traditional business models and assess their future viability, however successful they may be at present. Competition between business models is increasingly replacing differentiation based on products or process excellence [50].

#### Dependencies

*10.1. Technology Priority: Data as a Competitive Advantage for* Europe*:* In order to use data as a competitive advantage for Europe, the data sharing business models for individual companies in Europe need to be elaborated.

*10.2. Technology Priority: Data Spaces and* Networks*:* Data spaces and technical networks must be available to enable data sharing business models and create a playing field for fair competition.

#### Relevant use cases / application domains

Business models within a given value network can exemplarily be based on the St. Gallen Business Model Navigator [51] as depicted in Figure 5, showing an example of an IIoT value network with the respective business and role relationships. The use of IIoT platforms is often based on a value

network. However, industry not only focuses on selling products to their customers and users but on collecting information about the use of the products across their entire lifecycle. The latter allows the industry to tap into added sources of revenue by offering data-driven services and obtaining feedback on how to improve the product. IIoT platforms support this goal with a technical implementation that may be open source based.

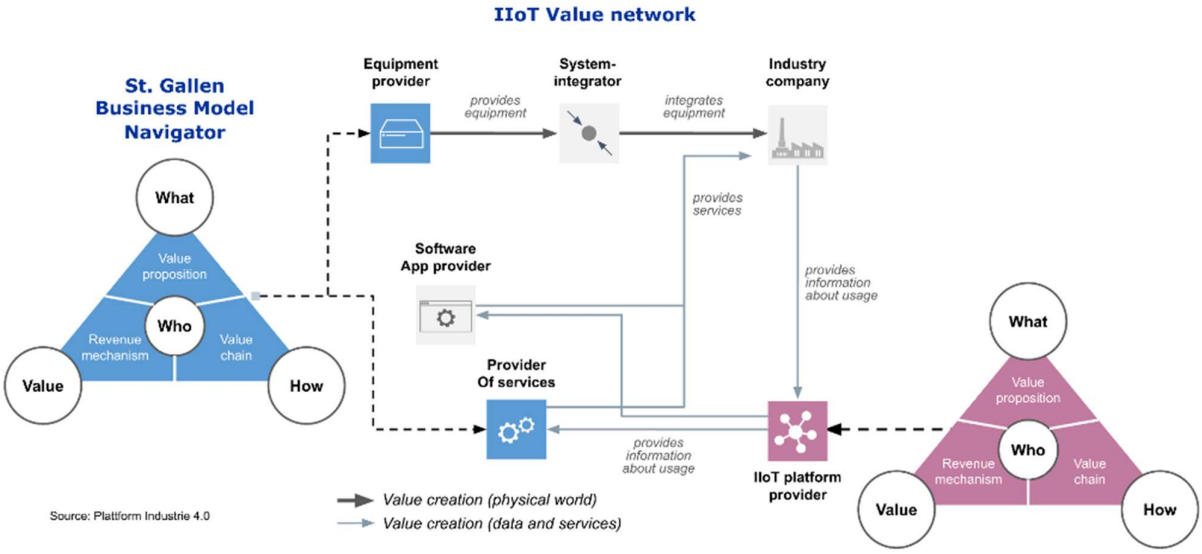



*Figure 5: IIoT Value Network overview*

Examples of real projects under development that establish data spaces to create real data businesses along new value chains, are Catena-X [18], the Smart Connected Supplier Network (SCSN) [20], or EONA-X [21]. These projects use open standards and open source software like the AAS (Asset Administration Shell) [30], the Edata centre (Eclipse Data Components) [52], and data space technologies provided by other organisations like Gaia-X. The DPP (Digital Product Pass) project [53] gains momentum as it is building on top of previous projects like PCF which started measuring the Product Carbon Footprint [46] using AAS technologies.

### *Recommendations*

| | |
|---|---|
| *Short-term* | Create an integrated view of the technology, commercial (business model) and legal aspects and identify barriers, especially those which result in the need for cooperation between competitors; Competition Law, a simplification of multi-sided competition law regulations. |
| *Mid-term* | Integration of technology, commercial and legal assessments to provide an environment which does not create artificial barriers for multi-sided business and market activities based on clear rules (e.g. for data sharing) to provide a secure legal framework for cross-vendor data sharing, whilst maintaining an open and competitive market. |

| | |
|---|---|
| *Long-term* | Expanding and aligning with global organisations to ensure eye-level market access and operations for large enterprises as well as SMEs globally requires harmonised rules in Europe and a legal framework that copes with the main market developments on a global scale. |

# SECTION 2: OPPORTUNITIES AND CHALLENGES OF DIGITAL SOVEREIGNTY

Digital data and related data processing make up a crucial cornerstone of the 2030 Digital Decade strategy [55], as also reconfirmed by the European Declaration on Digital Rights and Principles and the related Digital Decade Policy Programme 2023 [56]. Data is the common denominator. However, the increasing use of data processing and related computing technologies such as cloud, edge, and far edge computing, are promoting and enabling data exchange, analysis, processing and storage, but current operations and implementations do not generally meet the minimal threshold for digital sovereignty and are not yet regulated by formal and standardised policies.

Digital sovereignty is omni-present. It intervenes: (i) *on the entire life cycle* of the systems, the data, and any data processing (see the *Annex* to this Roadmap), (ii) before and during *strategic* venturing, partnering, investing in knowledge, talent, cash and kind and other collaborations, (iii) before and during procurement, sourcing, development, production, integration, building and implementation, (iv) before and during deployments and ongoing operations and upgrading, (v) during *scheduled and unscheduled events* and maintenance, incidents, attacks by malicious actors, recovery, further hardening and improvements, and (vi) when preparing and implementing any re-use, switching, recycling, up-cycling, or decommissioning. Digital Sovereignty [57] creates, identifies, defines, loads, and otherwise nuances a vast set of notions, principles, dimensions, perspectives, and other related requirements to come to the appropriate digital sovereign levels of data processing and related data processing infrastructures in Europe aimed for by the Alliance as set forth in its Terms of Reference, the strategies concerning the EU Fit for the Digital Age, Digital Decade 2030 targets, data cybersecurity and others.

In this context, technical sovereignty is linked to the ability at European level to act and decide independently in a global environment on edge and cloud services, systems, and technologies. It benefits the development of strong competencies, research and innovation, the promotion of the European industrial position on edge and cloud, and the protection of European values and democracy. Policies aiming at greater European autonomy and technical sovereignty for edge and cloud services should analyse the different digital components at hardware, software, data, and architecture level taking into consideration the different phases related to research, trial, design, production, operation, and use. Some components are harder to tackle from the sovereignty point of view (such as microchips and raw material), while others are lower hanging fruits (e.g., software (open source or otherwise), data architectures, data components and governance). More about the opportunities and challenges of digital sovereignty are cited in the *Annex* of this roadmap.

Achieving and sustaining digital sovereignty, while simultaneously addressing societal concerns and facilitating innovation of new digital value models, business and financial models, is a challenge. It depends on the availability of the necessary technological and organisational (public,

private, societal and interdisciplinary) capabilities to exercise the appropriate levels of sovereign control over how assets, means and values are used. The strategy to secure digital sovereignty needs to ensure that Europe has its own capabilities in the areas of (amongst others): (i) infrastructure that provides the basis for trustworthy data processing, digital devices, systems and services, (ii) software and platform stacks that allow the processing of services and data, and, (iii) technical, legal and organisational safeguards and measures for dynamic assurance, accountability and related controls against bias, misuse, manipulation, concentration risks, surveillance, related security issues, and other possible social and economic disruptions. This is not a one-time exercise but will need to be at the forefront of our minds continuously, as will the dynamics of technologies, markets, geopolitics, the climate, supply chains, and society.

## Focus Area: Build, Achieve & Sustain Digital Sovereignty

Continuously considering, building, achieving, and sustaining digital sovereignty brings challenges and opportunities. To address those challenges and grasp the opportunities, the joint development priorities in the following paragraphs have been identified. The figure below provides an overview of those seven (7) highlighted priorities needed to build, achieve, and sustain digital sovereignty. These are described in the following paragraphs in random order, as each stakeholder within the EU (public, private, research, academia, societal, and otherwise, and whether at local, regional, national, or Union level) will have perspectives that may lead them to start with one priority, with a set of priorities, or with multiple priorities in parallel.


*Figure 6: Highlighted priorities to build, achieve & sustain digital sovereignty*

## 2.1. Technology Priority: Landscape Sovereignty-enabling European Digital Capabilities

### Key drivers

For more than a decade, the EU has already been allocating massive amounts of resources and funds to programmes and projects focusing on or otherwise addressing emerging technologies, systems and other digital capabilities related to digital sovereignty and related challenges. However, there is no clarity, overview, or useful insight available about whether and to what extent project results are concrete, useful, viable, effective, and sustainable to add to the building, achieving, and sustaining of European digital sovereignty.

Having a clear, practical, and otherwise useful landscape of the EU-funded project deliverables and outcomes is required. It can provide oversight and insight into what has already been done, where it can be usefully deployed and further developed, and what is still missing. Just mapping those geographically is not enough; the various deliverables and results – and, where available, post-project dissemination activities – will need to be judged on their merit. The other main goal is to identify synergies, gaps, and improvements, and to use these for consideration for (further) investments and related activities. Where possible, one can also consider inviting, assessing, and, where appropriate, adding the deliverables and other results from similar projects of Member States or regions as well.

What is missing refers to a useful mapping of the identified technology deliverables, their results and other results to the extent deemed sufficiently concrete, viable, effective, TRL-matured, governance-ready, market-ready, and/or sustainable to add to the building, achieving, and sustaining of European digital sovereignty. Such mapping needs to start with structured visualization of identified domains and dimensions of (to be assessed and otherwise collaboratively and multi-angled plotted and mapped) research activities, innovation activities, and related products, systems, services, or other capabilities of European organisations that are active in the cloud and edge computing domain. Thereafter, synergies, gaps, and improvements can be identified and used for various purposes, including for consideration for (further) investments to facilitate the building, achieving, and sustaining of European digital sovereignty. For such vetting purposes, for instance, the various aspects of the evaluation components and queries of the European Innovation Council and related lessons learned could be considered and optimised for the purpose and particulars of the mapping and plotting described above.

### Dependencies & relevant use cases / application domains

Digital sovereignty is an omni-present dimension and is at the heart of both the EU Alliance as well as relevant EU policy initiatives, including the Digital Decade 2030 and its Digital Decade Policy Programme 2030. As such, digital sovereignty is an essential dependency to any other priority, and is also, vice-versa, dependent on how and to what extent digital sovereignty has been considered,

designed by default, implemented, monitored, and continuously kept up to date. The same applies for the use cases and application domains. Additional references are cited in the Annex.

### *Recommendations*

| | |
|---|---|
| *Short-term* | A cross-EU initiative is necessary on the one hand to map and plot the landscape of EU-funded project deliverables and digital competences and capabilities developed, and on the other hand to map the various identified market needs, technical developments, climate (change) developments, geopolitical developments, and policy developments. This mapping should mainly focus on the outcomes that are relevant to cloud, cloud-to-edge, edge computing, data management, and data processing. These could be, for example, linked with the Open Research Europe initiative launched by the Commission, while focusing more on and catering for go-to-market oversight and insights for EU organisations. The goal is to tackle both the manufacturing, supply, provider-side, and the procurement, customer, user-side, as well as the people and societal-side at large. Within such mission and scope, it is proposed to analyse: (i) identified and initially addressed societal challenges and related value model cases, use cases, business models and financial models, (ii) technical, legal, organisational, and operational capabilities and competences, (iii) data, data classifications, data architectures, data spaces and related knowledge, expertise and tooling, and (iv) skills and competences of existing, future, and otherwise relevant stakeholders and workforce. |
| *Mid/long-term* | Based on the mapping and plotting outcomes of the short-term activities (i.e. knowing what viable deliverables and other results are already readily available, knowing how and with whom to operationalise, deploy, and sustain those, including knowing where and how to join forces), it is proposed to invest in vetting synergies, gaps, and improvements among the European digital capabilities based on current and anticipated market needs. Afterwards, this insight and oversight will be used for the determination of (further) investment areas. For the avoidance of doubt, this also means that development and other innovations are furthered, applied, deployed to, and sustained in the market - and are not left behind. These development and other innovations should be of Technology Readiness Levels TRL6 and TRL7. |

## 2.2. Technology Priority: Narrow the Investment Gap & Other Resources Gap

#### Key drivers

While early-stage technology companies and other tech ventures, including but not limited to cloud and edge computing companies, are being heavily funded in other parts of the world, this is

not the case in Europe. The business angle and other venture capital by Europeans or European organisations as well as subsequent financing by European organisations (e.g. public or private) is at a dangerously low level within the European Union. The European Union, its Member States, and related sectors and organisations are outspent and outsmarted substantially. European grass-rooted initiatives, ventures, or businesses, whether early-stage, SMEs, entrepreneur or otherwise, currently stand no chance of remaining truly European if they have the ambition to become a significant market player. In that context, they are acquired and actually become non-European so as to seriously grow, scale and become champions in their respective markets. This clearly undermines European digital sovereignty.

The need is to support European companies and other ventures with technology solutions and capabilities that the global markets desire and pay for, but which can also grow, scale, and succeed within the European markets and sectors by remaining truly European. One of the main components is to narrow the investment gap. To this end, the mapping between the currently fragmented and seemingly not-orchestrated public and private investments in the EU and its Member States is missing. Teaming up from a shared perspective of European digital sovereignty starts with transparency of and appreciation by the relevant stakeholders – which are not merely financial investors, whether public or private, and their respective and various values, perspectives, needs, and interests. Such insight and oversight lead to sufficient levels of transparency, trust, willingness, comfort, and execution power. The latter is necessary to identify and discuss if, what, and to what extent European synergies, investments, and returns on investment should be considered and directed towards deployment, nurturing, and monitoring.

It should be noted that merely making available a substantial amount of structural and ongoing financial investments will not lead to success in terms of European digital sovereignty. Following solid financial investment, vital non-financial and other qualitative attention is necessary. The qualitative objectives, values, coordination, governance, returns, and other interests need to be very clear on a detailed level and need to be continuously optimised as per the dynamics in the current digital age. Focus may be put on one domain or risk-dimension at a time to learn, pivot, and improve, while architecting and preparing various relevant scenarios of potential events / occurrences that may arise in each domain of European digital sovereignty.

### Dependencies & relevant use cases / application domains

Digital sovereignty is an omni-present dimension, and at the heart of both the EU Alliance as well as relevant EU policy initiatives, including the Digital Decade 2030 and Digital Decade Policy Programme 2030. As such digital sovereignty is an essential dependency to any other priority, and is vice versa dependent on how and to what extent digital sovereignty has been considered, designed by default, implemented, monitored, and continuously kept up to date. The same applies for the use cases and application domains. Additional references are provided in the Annex of this Roadmap.

### *Recommendations*

| | |
|---|---|
| *Short-term* | Bridging the main cross-EU investment initiative will start with mapping and plotting the various landscapes and meta-landscape, and their respective stakeholders. This effort needs to be supported by the identification of the values and interests of the stakeholders and their respective expectations of investment returns. Meanwhile, relevant scenarios, business and financial models will be architected to identify the various benefits and preconditions and establish the appropriate net benefits that are envisioned. |
| *Mid/long-term* | Insight and oversight will grow to a level where these can be operationalised and deployed. Starting relatively modestly yet in a way that can grow, agility to evolve and be improved is recommended. As appreciation within the EU is sought after, interest, willingness and determination to invest and alignment to investments are expected to increase. Further organising, executing, monitoring, and improving are essential. |

## 2.3. Technology Priority: Operationalize Europe's Championing of Human-Centric & Other People-Centric Values

#### Key drivers

In the digital age and because of globalization, the EU is generally seen as a leader of human-centric and other people-centric values such as those implemented in the various EU strategies adopted in-line with the digital transformation objective. An example of this is the GDPR. This human-centric and data-centric regulation developed in-line with the EU digital transformation objective has inspired many countries around the world. However, the EU's normative power alone cannot guarantee European digital sovereignty for its citizens, businesses, organisations, society, and economy; nor can it guarantee that human-centric and otherwise people-centric policy instruments give the EU, its Member States, citizens, and organisations a competitive edge in the EU and abroad. Other examples are the Digital Markets Act (DMA), Digital Services Act (DSA), Network and Information Security 2 (NIS2), (proposed) DORA (Digital Operational Resilience), (proposed) electronic IDentification, Authentication and trust Services 2 (eIDAS2), (proposed) Interoperable Europe Act, (proposed) CER (Resilience of Critical Entities), (proposed) Data Act, (proposed) Cyber Resilience Act (CRA), (proposed) AI Act, (proposed) AI Liability and other recent and upcoming policy instruments.

The objective is to leverage the human-centric and other people-centric values approach to a level that can be operationalised, monitored, and enforced – also by citizens and organisations themselves within the Rule of Law, in an EU-wide clear and transparent way. This will also export frameworks, good practices, and lessons learned beyond the EU, and enable to market these value-centric digital products, systems, and services abroad. It will strengthen both the digital sovereignty

within the EU as well as other countries and regions in the world. Furthermore, it will bring benefits to the European private sector, as more human-centric and otherwise people-centric digital products, systems, and services can be exported or otherwise offered to (respectively can be procured from) a global market with the same or similar digital sovereignty objectives.

Towards the achievement of the aforementioned objective, it is required to identify, map and plot Member States, regions and other states that have been inspired by and are implementing various EU policies and strategies. The GDPR is one example of human-centricity, while also being the most mature to focus on. Furthermore, it is required to identify and where feasible deploy and monitor improvements to means, measures and related metrics, and other policy instruments to enable European citizens, communities, and other stakeholders to enforce their respective rights more effectively or help enforce the respective rights that are so essential for digital sovereignty.

### Dependencies & relevant use cases / application domains

Digital sovereignty is an omni-present dimension, and at the heart of both the EU Alliance as well as relevant EU policy initiatives, including the Digital Decade 2030 and the Digital Decade Policy Programme 2030. As such, digital sovereignty is an essential dependency to any other priority, and is vice-versa dependent on how and to what extent digital sovereignty has been considered, designed by default, implemented, monitored and continuously kept up to date. The same applies for the use cases and application domains, being applicable to all of them. Additional references are provided in the Annex of this Roadmap.

### *Recommendations*

| | |
|---|---|
| *Short-term* | The deployment will begin with the identification, mapping and plotting of human-centric values adopted by the Member States, regions, and local communities, since digital sovereignty starts with sovereign citizens, communities, and local society. This identification will facilitate communication, connection, and education regarding the choices made, lessons learned, and improvements planned, and will allow for efficient and transparent monitoring or enforcement. |
| *Mid-term* | Once the identification of human-centric values across the EU is completed, policies, legal instruments and good practices based on the human-centric values will be developed. These policies and frameworks will be standards for the manufacturing and the provision of services across the EU. |
| *Long-term* | These instruments, frameworks, and good practices as well as the digital products and services developed accordingly will be used as inspiration for other countries and regions in the world. |

## 2.4. Technology Priority: Organise EU Standards on Pre-procurement of EU Products, Systems & Services

### Key drivers

Digital ecosystems, cloud, edge and far edge computing, Internet of Things, distributed ledger technologies, AI, robotics, cybersecurity, and data management are what organisations are talking about daily and are increasingly assessing the opportunities, benefits, and risks of these. Technology makes innovation possible, and technology is a must-have in organisations, society, and the economy. It is essential for the successful and future-proof operation of an organisation. It can be the difference between an incumbent with no future continuity and no relevance, and one that is ready for the future. However, given the increasing dependability on and complexity of digital technology and digital ecosystems, most organisations do not know what they need, what to procure, and how to procure it. The latter includes all relevant elements, components, functionalities, and non-functional aspects (such as security, safety, privacy, resilience, and accountability) to create their own digital sovereignty, and augment the digital sovereignty of their sector, market, Member State, and as a result the digital sovereignty of the European Union. Meanwhile, especially in the European Union the existing OT and IT legacy and their life cycles are relatively large and further complicate catching up and keeping up.

European organisations need to have dynamic pre-procurement and procurement capabilities that can facilitate successful engagement between organisations, vendors, staff, customers, and society. This will enable European organisations to make informed decisions on what they need, what to procure (pre-procurement), how to procure it, how to negotiate such technology arrangements (such as platforms, digital ecosystems, networks, and technology-as-a-service) and how to keep it optimised and to continuously monitor it. The same applies for the essential and various combinations of digital functionalities, non-functional aspects, and capabilities that make up a digital ecosystem, platform, product, or service. These efforts will enable organisations both to become and stay more resilient and competitive, and to support their digital sovereignty and the sovereignty of their network, sector, Member State, and the EU. Furthermore, the aforementioned efforts will facilitate the creation of a decision model that helps to ensure compliance with regulatory frameworks and industry standards and, thus, facilitates trust and trustworthiness.

### Dependencies & relevant use cases / application domains

Digital sovereignty is an omni-present dimension, and at the heart of both the EU Alliance as well as relevant EU policy initiatives, including the Digital Decade 2030 and its Digital Decade Policy Programme 2030. As such, digital sovereignty is an essential dependency to any other priority, and is vice-versa dependent on how and to what extent digital sovereignty has been considered, designed by default, implemented, monitored and continuously kept up to date. The same applies for the use cases and application domains. Additional references are provided in the Annex of this Roadmap.

### *Recommendations*

| | |
|---|---|
| *Short-term* | Common reference models concerning the appropriate levels of performance, cybersecurity, data protection and data management, and negotiation capabilities will be determined. Based on these models, good practices and/or methodologies on how to conduct pre-procurement and procurement of digital products, systems, and services will be developed. In the short-term, relatively modest deployment is recommended to start with, for instance in a certain sector or a certain group of organisations. |
| *Mid-term* | Focusing on certain sectors or groups of organisations is recommended to help increase both the appreciation of these pre-procurement capabilities as well their competitiveness on the market, including mitigating becoming an irrelevant market player, and their ability to offer European, superior, state-of-the-art products, systems and services and the resulting increased consumer and other market trusts. |
| *Long-term* | The more challenging sectors, or groups of organisations can be enabled and helped to deploy these pre-procurement capabilities, including structured, modular architectures, data-centric, technology and vendor-neutral and by-design approach following the most demanding regulatory frameworks and industry standards. |

## 2.5. Technology Priority: Make EU Regulations fit for a Digital Sovereign Europe

#### Key drivers

Despite the indisputable benefits of the digital age for individuals, organisations of all sizes, Member States, and society at large, the digital age also raises risks of critical importance within the Rule of Law such as the complexity in attributing responsibilities. The level of dependability and the level of ever-increasing dynamics justify that and it is proven daily. It is challenging the digital sovereignty and the Rule of Law, both on a European level and on the Member States level. This leads to many challenges to address, risks to mitigate, detrimental impact to avoid, re-organise/coordinate and orchestrate mitigation of detrimental consequences and related responsibility, accountability, liability, and enforcement capabilities, as well as renewed/improved monitoring and supervising. In this context and towards protecting vital societal interests, European regulators have been focusing over recent years on how best to protect the interests of individuals acting under multiple personas (e.g. data subjects or consumers), business interests of organisations (e.g. trade secrets) and the interests of Member States, focusing also on how best to protect critical infrastructures (e.g. hospitals) and products (e.g. IoT devices). While the European regulators have already presented various legislation proposals, most of them still give Member States discretion in certain areas. This has resulted in diverging approaches and fragmentation that

has subsequently created challenges for conducting cross-border business and innovation with regards to new technological developments and cybersecurity solutions.

While the existing policy instruments, the efficiency of enforcement, and the existing legal structures, responsibilities, measures, remedies, and other capabilities are challenged, these can be improved in a transparent and accountable way. Furthermore, the intertwined facet required in the digital age refers to a convergence of regulatory approaches across the Union and, therefore, the new EU regulatory landscape for emerging technology should not give Member States discretion or at least not in certain areas.

Focusing digital ecosystems in multiple sectors, and how to go from a trusted and trustworthy single component to a trusted and trustworthy end-to-end system, where multi-use (other than a single intended use approach) – including unintended use – is required. This needs to be supported by strengthening digital sovereign authorities, such as national data protection authorities, cybersecurity authorities, and competition authorities. The digital sovereign authorities will exploit transparent and trustworthy digital means to operate independently yet accountably (while addressing the fault-lines between privacy and freedom, and surveillance and national security) in accordance with their mandate. Furthermore, new regulatory frameworks should adopt data-supported transparency and accountability in contracts regarding digital products, systems, and services for the benefit of Member States, citizens, society, and economy within the Rule of Law.

This could be provided by introducing general security and safety principles, common risk assessment framework, generic cybersecurity controls and measures in horizontal regulations (such as the Cybersecurity Act, Radio Equipment Directive, General Data Protection Regulation, General Product Safety Directive, eIDAS Regulation, Sales of Goods Regulations and NIS2 Directive, but also the proposals the AI Act, Data Act, Cyber Resilience Act, respectively revised liability and safety directives, i.e. the Product Liability Directive, General Product Safety Directive and Machinery Regulation). However, these efforts should avoid overlaps, confusions and conflicts between specific vertical regulations (e.g. Medical Device Regulation), regulatory standards (e.g. RTS or the Second Payment Services Directive 2). Moreover, enforcement capabilities of regulatory authorities should be clarified and strengthened in the respective markets such as what applies to whom, what prevails, how to address conflicts, and who is allowed to enforce what.

### Dependencies & relevant use cases / application domains

Digital sovereignty is an omni-present dimension, and at the heart of both the EU Alliance as well as relevant EU policy initiatives, including the Digital Decade 2030 and its Digital Decade Policy Programme 2030. As such, digital sovereignty is an essential dependency to any other priority, and is vice-versa dependent on how and to what extent digital sovereignty has been considered, designed by default, implemented, monitored and continuously kept up to date. The same applies for the use cases and application domains. Additional references are provided in the Annex of this roadmap.

### *Recommendations*

| | |
|---|---|
| *Short-term* | Having a clear picture (oversight and insights) of the various legal relationships in the development, implementation, delivery, maintenance, and sustainability (and other life cycle phases) of a system, product, or service will be required in order to understand the perspectives of the legal positions of each of the relevant stakeholders. While service and sale contracts may claim that they are only applicable to one separate part of a product or service, this does not apply in the digital age. A part of the system or a separate layer cannot be considered to function independently of the remaining parts or other layers, i.e., without affecting the whole ecosystem. However, to provide sufficient transparency and accountability, consumers and organisations (both private and public) will have an accurate and transparent account of how the technical layers and related dimensions (i.e. data, human, and identity), interact with their respective contractual/other legal documents, as well as which stakeholders are relevant (not only active) in each of those. The consumer or organisation will be able to identify the parties upon whom the service is dependent and who are the processors and sub-processors of data. Not only will this information provide the customer with greater transparency, it will also establish the extent of liability of various suppliers should a problem arise that requires legal redress. |
| *Mid-term* | Once transparency and accountability principles are well-placed in contract, several questions will be addressed. These questions arise from the use of advanced IT services and products, such as the liability for actions of IIoT devices that can make autonomous decisions and enter into legally binding agreements with third parties (e.g. connected home appliances purchasing products from third parties). The traditional understanding of property is static and it will likely change and respond to the dynamic nature of IIoT devices that can evolve and mature over time. It is also important to consider the status and the role of the customer in the ecosystem. It has been argued that two further distinctions of legal consequence can be made that are particularly relevant for consumers. |
| *Long-term* | More complexities in contracts will also arise in the context of clauses relating to the selection of jurisdiction. Most commercial contracts explicitly stipulate applicable law and jurisdiction governing them, to the maximum extent permitted by law. However, in cases where mandatory national laws apply, judges and/or the national competent authorities will have to abide by those. Therefore, cases may arise in which the judge and/or the national competent authority will have to apply different pieces of legislation, for example, to the same product. Thus, fully integrated rules on technology contract across the EU will be required and are recommended. |

## 2.6. Technology Priority: Support Distributed & Interoperable Architectures

### Key drivers

Data processing, in particular cloud services, is today characterized by a wide use of centralised architectures offered by a few global actors that have access to a huge amount of European data. Due to the dimension of these actors and the extended and vertical integrated offers aiming at embracing the different needs of customers, there is a lock-in effect stifling innovation and otherwise leading to low competition, difficulties, and obstacles when customers wish to change providers. In such context, European organisations, public, private, and otherwise, are penalized and are struggling to enter the cloud, cloud-to-edge, edge and other data processing market regardless of the quality and high levels of ethics, integrity, and trustworthiness of their services.

A more dynamic and competitive market of data processing should be a European objective, allowing innovation to emerge and the provision of different services with higher quality characteristics using a more distributed, interoperable, and multi-vendor cloud, cloud-to-edge, edge, and data processing infrastructures. A capillary deployment of interoperable edge nodes will allow distributed data processing and storage capabilities ensuring better performance, enhanced security, more social inclusion, and amplified industrial competitiveness.

### Dependencies & relevant use cases / application domains

Digital sovereignty is an omni-present dimension, and at the heart of both the EU Alliance as well as relevant EU policy initiatives, including the Digital Decade 2030 and its Digital Decade Policy Programme 2030. As such, digital sovereignty is an essential dependency to any other priority, and is vice-versa dependent on how and to what extent digital sovereignty has been considered, designed by default, implemented, monitored and continuously kept up to date. The same applies for the use cases and application domains. Additional references are provided in the Annex of this Roadmap.

### *Recommendations*

| | |
|---|---|
| *Short/mid-term* | In line with the Digital Decade objectives [58] and targets [59] for 2030 and European initiatives to foster digital sovereignty, decentralised architectures with distributed data processing and storage should be promoted, constantly expanding cloud-to-edge and edge capabilities and related interoperable infrastructures. The process for the authorization and allocation of funds should be leaner and faster in line with the speed of technological evolution with a clear timeline and clear roles and responsibilities among the institutions involved. |

## 2.7. Technology Priority: Promote & Implement Local Processing of Data

### Key drivers

It is important that data are appropriately protected in accordance with European values and regulations. A huge amount of European data is currently available to and processed by a few non-EU companies based in countries with different legislations, making it difficult to apply and enforce European legislation and to preserve European privacy and security standards.

Data is one of the components of technical sovereignty on which Europe can act. Data sovereignty can be addressed based on different layers, and the level of sovereignty can vary according to which layers we want to tackle given the specific scenario: (i) the *privacy layer* focuses on data and their data controllers who have control and primary rights to that data, and a sub-layer of protection can be identified keeping data safe and visualizing data location and access, (ii) the *residency layer* addresses the need for data to be moved according to specific rules and processes to be confined within a geopolitical boundary when at rest, (iii) the *locality layer* refers to a technology that requires it to be physically located within a geopolitical boundary so that no part/component of the technology is located elsewhere, (iv) the *authority layer* controls who can make decisions regarding cloud at large, including services and application, infrastructure, and platform components and assets, and (v) the *control layer* encompasses legal boundaries of control over services and applications, infrastructure, and platform components and assets.

### Dependencies & relevant use cases / application domains

Digital sovereignty is an omni-present dimension, and at the heart of both the EU Alliance as well as relevant EU policy initiatives, including the Digital Decade 2030 and its Digital Decade Policy Programme 2030. As such, digital sovereignty is an essential dependency to any other priority, and is vice-versa dependent on how and to what extent digital sovereignty has been considered, designed by default, implemented, monitored, and continuously kept up to date. The same applies for the use cases and application domains. Additional references are provided in the Annex of this Roadmap.

### *Recommendations*

| | |
|---|---|
| *Short/mid-term* | Depending on the sovereignty layer that is impacted for the data, the following recommendations are proposed:<br>• *Privacy layer* related to Data Control, Data Access, Data Use, Processing, Management & Protection: Operators and other data processors cannot access or view the data, in fact the concept of HYOK (hold your own key) is applied, ensuring encryption keys are held solely by the client by default, with the right to entrust certain key management to a trusted custodian while keeping in control over those keys. In order to ensure compliance with local privacy regulations per jurisdiction and/or local regional regulations (e.g. |

GDPR), audits on data governance are recommended. Moreover, access by external authorities will be avoided.

- *Residency layer* related to movement and rest: When ensuring sovereignty for movement of data and their treatment when at rest, it is recommended that services are running locally or at the regional periphery (while considering workload and related computing and sustainability optimisations elsewhere) and that data at rest are stored there (while considering fall-back and other disaster recovery scenarios), within a specific and specified storage. Customers can appeal and request sanctions for non-agreed data movement by the cloud/edge/data provider, who should operate on the bases of agreed data movement which can be tracked and documented. A line of sight between accountable parties should be granted.
- *Locality layer* related to physical location: The concept of end-to-end local data transfer should be introduced including, but not limited to, cloud infrastructures (tenants, storage) running locally. A set of cloud services should be delivered in an isolated (potentially air-gapped) fashion, while the control plane will be under local jurisdiction. Action enforcement will not be under the cloud/edge provider umbrella, but instead in charge of partners. SLAs and support will be managed locally.
- *Authority layer* (Decision Rights): As with GDPR, security certifications need to be managed at EU level (and where still required at regional or Member State level).
- *Control & Governance layer* (Ethical, Governance & Legal Rights): Infrastructures and services have local or governmental owners or controllers who can grant local governance requirements and take decisions at a local level. Authority must be independent from outside influence.

In terms of data, at each phase of the lifecycle, relevant stakeholders must be identified and their access to and accountability for the data itself, metadata, and inference data must be clearly stated and regulated.

## Focus area: The Holistic Approach

Considering the recommendations set forth in the previous section and the opportunities and challenges of digital sovereignty as described in the Annex of this Roadmap, the two main holistic roadmap recommendations are highlighted:

- Plot and map the various relevant sovereignty-enabling building blocks, to identify and grasp opportunities and to address various challenges and scenarios, and
- Continuously monitor, update, and optimise the various relevant sovereignty-enabling building blocks before, during, and after design, development, and deployment.

# SECTION 3: CLIMATE POSITIVITY, RESOURCE EFFICIENCY, AND CIRCULAR ECONOMY

While cloud and edge infrastructures continue growing, the carbon usage needs to be reduced to meet the EU goal of climate neutrality by 2030 for the data centre industry in Europe. Information and Communication Technologies (ICT) facilitate other industry business cases to reduce their carbon usage; however, ICT need also to reduce theirs. This builds the challenge ICT is facing, estimated to quadruple from 2010 to 8000TWh/year in 2030 [60]. Edge is seen as an enabler for reducing carbon usage by cloud by minimising data-distribution and making edge smart by focusing on sustainability from the very beginning. This section will sketch out the roadmap for potential mitigations. From research outcomes and ongoing research efforts, sustainability should be an intrinsic part of application landscape design.

To avoid the consequences of irreversible climate change (as a result of humans' activities), industry is required to significantly reduce its emissions. With their increasing industry footprint, cloud and edge are significant contributors to global emissions, making up approximately 14% of global greenhouse gas emissions [61]. Irrespective of the total consumption, the expansion of cloud in Europe will result in significant energy efficiency gains compared to other alternatives, like on-premises or private clouds. The increased provision of cloud and edge services will aggregate workloads on public cloud / edge services across Europe. Cloud service providers can better scale and allocate workloads on optimised infrastructures, operated in energy-efficient and environmentally friendly data centres, instead of traditional on-premises data centres. It is worth mentioning that some investments are still needed to optimise data centres and infrastructure towards becoming even more environmentally friendly, as discussed also in Section 6 and Section 8 of this Roadmap. Furthermore, an optimal allocation of activities between centralised and edge nodes will bring additional benefits by optimising network data traffic and workload distribution.

In addition, both centralised cloud and distributed edge services have a crucial enabling role for energy savings in the economy since they contribute to the digitalisation of more traditional industry sectors such as manufacturing or logistics. Energy savings resulting from the application of digital technologies through solutions in energy, manufacturing, agriculture and land use, buildings, services, transportation, and traffic management are higher than the ICT sector's own footprint - estimated at 15 to 20% [61]. The deployment of edge cloud solutions will further accelerate this trend by enabling a wider range of use cases based on ultra-low latency infrastructure and the associated services.

Overall, a sizeable investment would allow the acceleration of the integration of cloud and edge digital infrastructures in energy systems and would place Europe in a leading position for energy and resource-efficiency. Measures could encompass the use of green hydrogen for energy storage, the deployment of energy efficient technologies such as liquid cooling, the optimisation of

recycling in the supply chain, and the research in new technologies such as distributed concepts, AI/ML and emerging storage technologies, positioning Europe in a leading position for carbon neutrality. These investments will support the goal of climate neutrality by 2030 for the data centre industry in Europe, and therefore complement the Climate Neutral Data Centre Pact self-regulatory initiative launched by the industry and in line with the European Commission's priorities [62]. Two main European initiatives are focusing on these aspects, the European Commission's Code of Conduct for Energy Efficiency in Data Centres [63], and the European Green Digital Coalition [64]. In this context, the European Commission can further support these efforts through the adoption of reliable sustainability criteria (KPIs) for cloud and edge data centres.

# Focus area: Circular economy

## 3.1. Technology Priority: Sustainability by Design

### Key drivers

Global challenges associated with the current raw material shortage crisis, due to the COVID pandemic and aggravated by the Ukraine conflict, are not only causing a rise in raw material prices but also have huge impacts on the industry in the EU due to its high dependency on external resources [65]. For example, in the case of the EU automotive sector: the production reductions due to COVID-19 amounted to 4.2 million vehicles, almost 23% of total EU production in 2019 [66], representing missed commercial opportunities of more than 110 bn € [67]. Moreover, the need to replace gas with other less favourable carbon generating fuels can make electricity less green especially in the short term.

Adopting ideas and solutions for the circular economy will improve resource efficiency and, in combination with sustainable practices, will contribute towards reducing the EU dependency on external resources. In this context, general data availability and interoperability is a critical aspect for decision making. Factors such as privacy concerns, the absence of data interoperability schemes or the lack of trustworthy traceability systems hinder the transition towards circular economy models. In this context, infrastructure and platform-related aspects (as discussed in Section 9) are quite relevant.

Concepts of the circular economy could help to solve the associated challenges. To strive towards sustainability schemes, the following activities are proposed: (i) adoption of life cycle engineering activities to improve products' eco-efficiency [68], (ii) innovative schemes for the adoption of effective circular strategies based on informed decisions, such as strategies concerning the end-of-life status on products or strategies for creating circular supply chain models based on data-enhanced traceability (transparency and accountability), (iii) establishment of appropriate metrics and parameters to optimise the products' lifecycle, (iv) development of digital platforms and data sharing solutions for the effective management of the circular products and production-systems

lifecycles [69], (v) leveraging of blockchain solutions to bring transparency, traceability (Tracking Energy Source), and accountability in Carbon Trading and Climate Reporting, leading to standardisation for Sustainability reporting [70]. There is significant attention on the carbon economy and the tokenization of natural resources, in which blockchain may play a pivotal role. As for the environmental impact of blockchain technologies, the industry is responding with a focus on positive climate action. Newer blockchains work via more energy-efficient consensus technologies (e.g. Proof of Stake). Ethereum 2.0 aims to be carbon neutral. If a blockchain solution is implemented using the traditional Proof of Work consensus algorithms, its energy consumption will surpass any benefits it brings. In case of other consensus algorithms like Proof of Stake, used widely for the modern blockchain solutions, the energy consumption and GHG emission will be lower or equal to BAU technology for a specific use case. In addition, there are several DAO (Decentralised Autonomous Organisations) and industry foundations working on new initiatives and features that enable environmental and regenerative finance.

The figure (Figure 7) abstracts the aforementioned aspects together with two enabling building blocks: data spaces and new ways of data storing. The reasoning is straightforward: for a sustainable future, data is a key part of digital solutions and therefore, European sustainability data-eco-systems should be encouraged. In today's data centres, storing data is among the most "electricity-expensive" aspects [71].

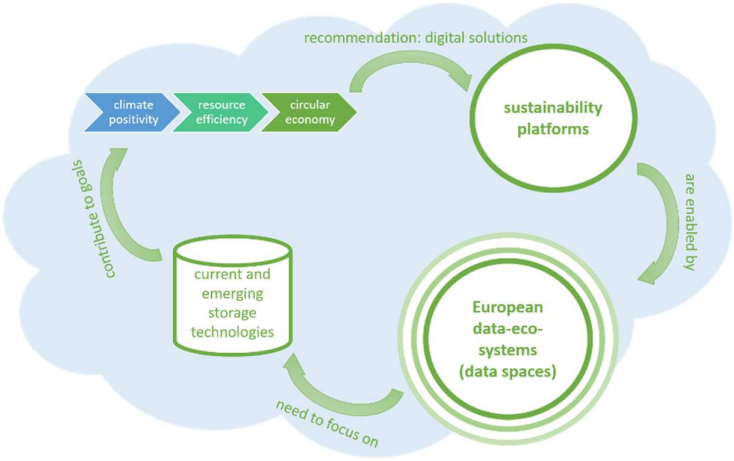



*Figure 7: Disruptive technologies to enable zero carbon cloud edge data storage & management*

## Dependencies

*Focus area: Innovative Design, Operation:* In order to achieve a stable circular economy state across the European cloud, edge, and telecommunication industry, the industry depends on successful developments and deployments in the design and construction of state-of-the-art data centre facilities.

*8.1. Technology Priority: Establish an Open Hardware* Ecosystem*:* Design and development of the used cloud foundation infrastructure should support ideas of circular economy. This should be the Open Hardware ecosystem including local manufacturing of the components, as also described in the *8.2.* Technology Priority: Print-And-Go, Implement Local Manufacturing for IT Equipment.

## Relevant use cases / application domains

Regarding use cases, serverless is a relevant enabler for all use cases listed in the roadmap. Representative ones are listed below:

The *cross-industry decarbonisation data platforms* use case is relevant in terms of facilitating the improvement of the visibility and control of greenhouse gas (GHG) emissions. Data platforms and data spaces will provide multiple industries with new services to reduce their emissions in line with increasing societal and regulatory requirements. Moreover, the combination of financial, performance, and emissions data is of major importance to ensure appropriate privacy and security. Thus, the cross-industry decarbonisation data platforms use case is strongly impacted by serverless technology, which enables an efficient use of resources at the time and place in which they are needed.

The *edge-to-cloud continuum / infrastructure* use case highlights several new challenges compared to standard distributed computing systems because of the heterogeneous computing environments, the heterogeneous and dynamic network environments, the node mobility, and the limited power capacity. Thus, the infrastructure technology use case related to the edge-to-cloud continuum is the one most affected by serverless architecture due to its scalability and portability across the continuum.

### *Recommendations*

| | |
|---|---|
| *Short-term* | Motivate component and system manufactures to provide information on used raw materials and potential composed materials. Collect this information in either data bases or better create a data space for that information in order to ease the actual data sharing across the industry. Support of the European Digital Product Passport normative activities using European standards like ASS by manufacturers. |
| *Mid-term* | Sustainability by design. Ensure that digital services deliver the required sustainability and environmental objectives, it is important to embed such design principles into the development of services from "cradle to grave". Solution providers will be encouraged to design future systems that are easy to repair, re-manufacturing and that can be reused during their life cycle. At the end of the lifecycle they will be easy to recycle. For future data centre and cloud/edge-related energy efficiency and sustainability regulations, the commissioning and decommissioning phases should be considered in addition to the lifecycle of an object. |
| *Mid-term* | Energy-efficient coding that reduces the effect of the software on the energy consumption of its hardware requires the push of existing best practices into European standards for sustainable software development. |

# Focus area: Data Decarbonisation

## 3.2. Technology Priority: Cross-industry Data Decarbonisation Platforms & Data Spaces

### Key drivers

By 2025, humanity is expected to produce 175 zettabytes of data [72]. Data platforms for cloud and edge that ensure both data and computational functionality are readily accessible and available. However, many organisations currently lack the necessary resources to properly manage the impact of their cloud presence on the environment. This is challenging in the long term, causing major preservation, cost, and sustainability issues. Europe should support research in disruptive technologies for data storage, management, and maximizing the value obtained from data to create impact.

Organisations require methods to automate data capture across the edge-to-cloud continuum and in order to reduce the effort associated with data gathering for environmental management. This will also improve the accuracy and level of insight achievable from the data, enabling overall emissions reduction and mitigating any increases resulting from data capture. Broad adoption of such systems will ensure that environmental data is easily and consistently included in business decisions.

The creation of Data Spaces through the federation of data platforms (as depicted in Figure 8) and the creation of associated governance frameworks will also offer a collaboration format for the consistent and managed exchange of data between organisations, further increasing the rate of decarbonisation. With the difference between the present global emissions trajectory and the rate of emissions required by science to avoid catastrophic climate change made clear, such an approach would make it possible for organisations to collectively identify and publish options to bridge this gap in the form of reduction opportunities. Companies could explore these opportunities and their feasibility, based on real information and results from other collaborators. This could include the latest market costs of implementation to identify the least cost-intensive means and ensure performance keeps track with science-based reduction targets.

The EU has already set up several initiatives to facilitate Data Spaces, which will support the creation of associated de-carbonization data platforms and their federation, such as GAIA-X, IDSA (Industrial Data Space Association), Catena-X, FIWARE, or BDVA (Big Data Value Association). Through these initiatives, many data platforms are emerging to collect and leverage data in the field of energy, mobility, smart-cities, manufacturing, healthcare, and others. By building on these initiatives, for example by ensuring consistency of sustainability data models and platform interoperability, and by pursuing the secure federation of sustainability data for cloud through data spaces, there is a strong opportunity for EU businesses to lead globally in this area.

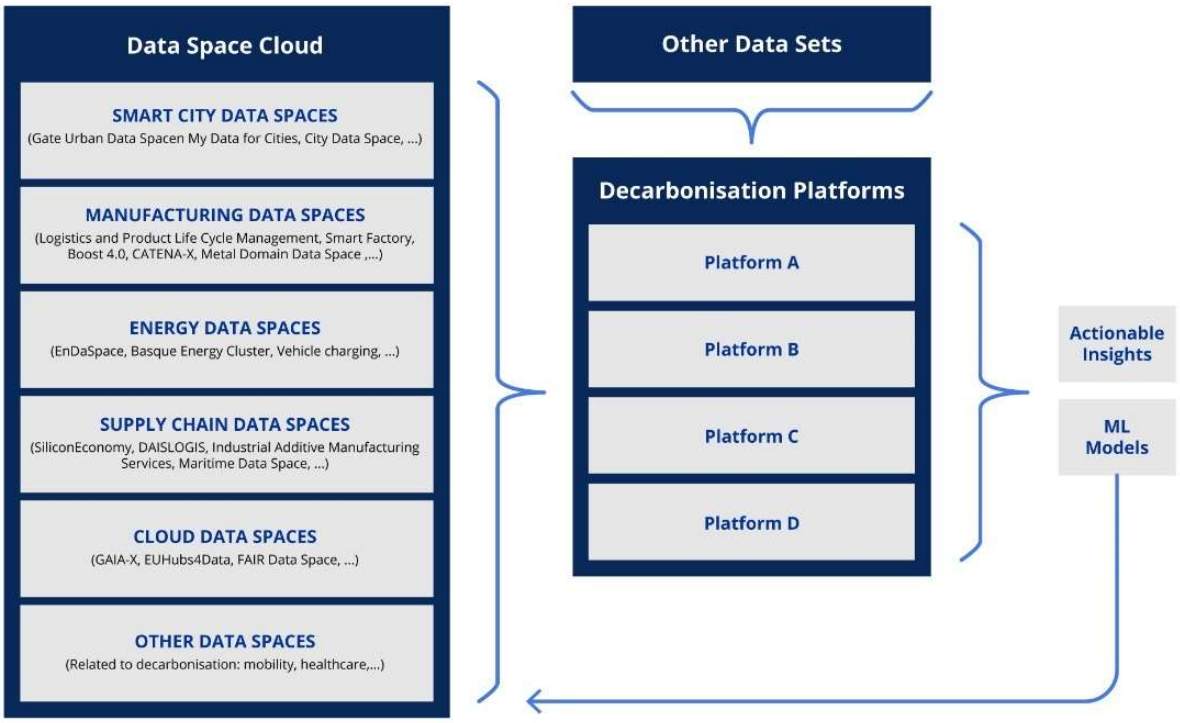



*Figure 8: Data platforms and data spaces*

### Dependencies

Several dependencies exist when it comes to the cultivation of Data Platforms and Data Spaces for cloud emissions management. The following technology priorities are prerequisites for cross industry decarbonisation data platforms:

*1.1. Technology Priority: Representation in Open Standards, Relation to Norms &* Standards*:* A set of standards for key cloud metrics and decarbonisation reporting are proposed and are required for the realisation of the proposed data platforms and data spaces.

*1.4. Deployment Priority: Data-Sharing Business* Models*:* To provide organisational awareness and adoption of data platforms where new commercial and technical mechanisms for data sharing facilitate sharing of decarbonisation data.

*5.1. Technology Priority: Open Standards for Cloud Infrastructure* Services*:* To facilitate availability of cost and emissions data at sufficient levels of granularity, such that buy in and action from business decision makers is increased. Additionally, open standards and data models should be pursued to ensure interoperability and adoption.

### Relevant use cases / application domains

Serverless is a relevant enabler for all use cases listed in the roadmap. Representative ones are listed below:

The *cross-industry decarbonisation data platforms* use case will improve the visibility and control of the greenhouse gas (GHG) emissions associated with cloud and edge consumption. Data platforms and data spaces will provide multiple industries with new services to reduce their emissions in line with increasing societal and regulatory requirements. Moreover, the combination of financial, performance, and emissions data is of major importance to ensure appropriate privacy and security. In this context, the cross-industry decarbonisation data platforms use case is strongly impacted by serverless technology, which enables the efficient use of resources at the time and place in which they are needed. Finally, decarbonisation of cloud and edge environments must be seen to be economically practical for adoption of sustainable best practices to take place.

Regarding the *technology* use cases, the infrastructure use case related to the edge-to-cloud continuum is the one that is most affected by serverless architecture due to its scalability and portability across the continuum.

### *Recommendations*

| | |
|---|---|
| *Short-term* | By securely federating data in cross-industry decarbonisation Data Spaces, many advanced emissions reduction strategies will be made possible, both in and beyond cloud-edge infrastructures. For example, the accuracy of carbon intensity measurement will increase and can be shared, finely tuned emissions factors can be identified based on location or device and fine-grained comparison of scenarios and emission reduction actions can be performed. A uniform system for multiple stakeholders would be capable of identifying buildings, business entities and others that are operating significantly less efficiently than others. The Product Carbon Footprint (PCF) European standardisation activities foster data interoperability along all value chains. A trust framework like the one developed by GAIA-X will secure the collaboration between stakeholder, and possibly make an emissions data economy achievable. |
| *Short-term* | Businesses need Data Spaces to underpin their Net Zero journeys by providing emissions data alongside data in support of their business cases. By ensuring business and emissions metrics are handled and presented together in holistic Data Platforms, the emissions impact will be considered in decision making and the business cases for emissions reduction activities will be made clearer with less effort. Functionality to forecast future scenarios, based on robust federated data sets, will further increase the confidence of investors in de-carbonizing initiatives. |
| *Mid-term* | Decarbonisation Data Platforms will evolve from basic reporting platforms to automated, real-time remediation platforms where events such as the breaching of a defined threshold will trigger actions or guidance to reduce emissions. H-Cloud's Cloud Computing in Europe [73] report emphasises the potential of cloud native workloads to move beyond the benefits of simple virtualisation or containerization, in order to leverage advanced cloud functionality for the |

| | |
|---|---|
| | purposes of decarbonisation. Basic actions will be possible, such as automatically shutting down an unused server, or, more interestingly, machine learning models will be utilised for more advanced decision making based on repeating trends or correlations in the data. Furthermore, the approach will be extended to the edge, where information collected in data platforms will be acquired at the edge level (e.g. in smart cities, factory floors, hospitals) to extend the scope of emissions management consistently across many devices. In addition to performance versus that of competitors, a platform would also be able to present performance compared to meaningful reduction targets, as dictated by science, such as those already adopted by the European Union. |
| *Long-term* | A standard data model and set of metrics for decarbonisation of industrial data, edge, and cloud should evolve for Data Spaces that allow decarbonisation to become a reality. Federation of Data Platforms and collaboration between participating organisations and institutions will both facilitate and benefit from a common data model for key metrics. Examples of such metrics include common standard emissions factors and the discrete elements of functionality to which they apply. Support and adoption of a standard data model from the EU initiatives mentioned will ensure data sets can be kept compliant while encouraging organisations themselves to maintain compliance. Moreover, through the data model, a significant leap in data sharing and analysis for the purposes of decarbonisation can be made. It will support the creation of new applications that leverage and promote the intelligent optimisation of cloud and edge resources while enabling best practices to be identified and replicated within all participating industries. |

# Focus area: Data Centre Considerations

## 3.3. Technology Priority: Code of Conduct for Energy Efficiency

### Key drivers

The European Code of Conduct for Energy Efficiency in Data Centres (or "Code of Conduct") [63] has been created in response to the increasing energy consumption in data centres and the need to reduce the related environmental, economic, and energy supply security impacts. The aim is to inform and encourage data centre operators and owners to reduce energy consumption in a cost-effective manner without hampering the mission critical function of data centres. The Code of Conduct aims to achieve this by improving understanding of energy demand within the data centre, raising awareness, and recommending energy-efficient best practices and targets. The Code of Conduct represents an annually evolving set of energy-related best practices covering the

physical building, mechanical and electrical plant, data floor, cabinets, IT equipment, operating systems and virtualisation, software, and business practices. Together they represent the latest best practices collated from a broad group of expert reviewers from operators and vendors to consultants, academics, and professional and national bodies.

It is important to note that the European Code of Conduct for Energy Efficiency in Data Centres is included within the technical screening criteria of the EU Taxonomy Delegated Act Technical Annex [74]. Additionally, the "Climate Neutral Data Centre Pact" is a self-regulatory initiative with the target of making data centres climate neutral by 2030 [75]. Data centre operators and trade associations are committed to the European Green Deal, achieving the ambitious greenhouse gas reductions of the climate law and leveraging technology and digitalisation to achieve the goal of making Europe climate neutral by 2050.

### Dependencies

*6.4. Technology Priority: Energy Optimisation and Resource* Conservation*:* In implementing the ideas of the Code of Conduct, for Energy Efficiency in Data Centres, data centre developers and companies as well as server manufacturers should be motivated to gear their developments towards energy-optimised operation. Furthermore, optimisations in operation should be made possible. In particular, technical advances should be easy to implement.

*6.1. Technology Priority: Optimised Data Centre Design for Edge and* Cloud *& 6.5. Technology Priority: Rethinking and* innovating Design for Sustainability*:* Investments should be made in the development of applications and systems for the innovative use of residual energy and energy storage for the edge and cloud data centres.

### Relevant use cases / application domains

The *edge-to-cloud continuum / infrastructure* use case highlights several new challenges compared to standard distributed computing systems because of the heterogeneous computing environments, the heterogeneous and dynamic network environments, the node mobility, and the limited power capacity. This use case is the one that is most affected by serverless architecture due to its scalability and portability across the continuum.

The *cross-industry decarbonisation data platforms* use case addresses the priority of improving the visibility and control of the greenhouse gas (GHG) emissions. Data platforms and data spaces will provide multiple industries with new services to reduce their emissions in line with increasing societal and regulatory requirements. Moreover, the combination of financial, performance, and emissions data is of major importance to ensure appropriate privacy and security. Thus, this use case is strongly impacted by the serverless technology that enables an efficient use of resources at the time and place in which they are needed.

### *Recommendations*

| | |
|---|---|
| *Short-term* | Encourage producers and users to disclose the raw materials and composed materials used to build components and systems based on the European Digital Product Passport. Develop and provide a database / data space containing information in order to enable users to take educated decisions and support reuse / repair / update during the system life cycle and recycle at the end of the life cycle. Operators, co-location providers, co-location customers, and Managed Service Providers (MSPs) should participate or leverage the European Code of Conduct for Energy Efficiency in Data Centres [76]. |
| *Mid-term* | Promote the alignment to the European Code of Conduct for Energy Efficiency in Data Centres and related standards, such as LEED, BREEAM etc. Facilitate approaches for reuse of data centre heat and techniques to modernise data centre infrastructures through carbon-neutral technologies. |
| *Long-term* | Foster the research and development of new technologies, for example Hydrogen-powered data centres and the integration in hydrogen grids. |

## 3.4. Technology Priority: Use of Digital Technology as AI/ML

#### Key drivers

Technologies such as artificial intelligence (AI) through machine learning have the potential to optimise, for example, the distribution of workloads in and outside the data centre, considering environmental and efficiency aspects. Parameters such as energy efficiency, green energy and data optimisation can be included in the necessary decision-making processes. It should be considered that the optimisation of the processes also requires resources, which have to be included in the end-to-end calculation. The aforementioned AI approaches can facilitate automated workload characterization and automated placement based on performance, green power efficiency, and the economical use of data and its storage space. Additionally, such approaches can be utilised for aligning energy management, energy production, edge application energy usage and peak handling on edge cloud and (I)IoT [77]. Digital twin simulations can also be exploited for dynamic, real-time data hall management, allocating IT space, or predicting the data hall conditions in order to save energy.

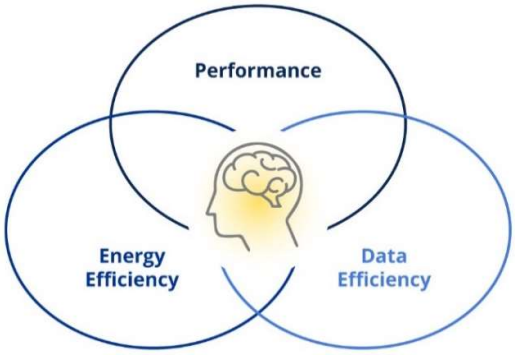



*Figure 9: Intelligent energy management [52]*

Data tends to be stored indefinitely in data centres without being reused. This trend is increasing with sensors that continuously generate data. This data may vary, evolve, and be less adapted to AI models or used over time. It therefore becomes useless to keep it indefinitely in energy-intensive storage spaces. Thus, it is important to filter the data to decide what should be deleted, archived, aggregated, or recycled.

Dependencies10.4. Technology Priority: IIOT/AI Applications. Data collection from IoT sensoring and assessment, and elaboration and usage by means of AI/ML tools as indicated in the short to mid-term recommendations below allows the enabling, unlocking and boosting of industrial processes improvements.

### Relevant use cases / application domains

Setting up actions as indicated in the short to mid-term recommendations is key to setting the baseline data vocabulary and tools for AI and ML to be able to provide benefits in any of the industrial use cases listed in the specific sector (Healthcare, Mobility, Logistics, Smart Cities, Sustainability, Supply Chain, Public Safety & Disaster Relief).

In *AI federated machine learning use cases*, one of the main concepts in the computing continuum is the use of caching to bring the intelligence closer to the edge, instead of leaving the intelligence centralised in cloud servers. Federated learning at the edge trains AI models across edge nodes without the need to transfer data to the cloud to enhance privacy preservation and bandwidth.

The *edge-to-cloud continuum / infrastructure* use case highlights several new challenges compared to standard distributed computing systems because of the heterogeneous computing environments, the heterogeneous and dynamic network environments, the node mobility, and the limited power capacity.

*Smart city* services optimise resource usage and improve the quality of life by connecting and utilising data from different sectors (e.g. power plant, utilities, infrastructure, health, mobility, etc.). As data processing is the enabler for smart cities, the digital infrastructure from edge to cloud is a key/critical success factor to provide the right data at the right time and to ensure Data/Digital Sovereignty.

### *Recommendations*

| | |
|---|---|
| *Short-term* | Research study to evaluate the current market situation and the impact of AI/ML on data centre energy efficiency. The main targets of the studies are: (i) evaluation of the current as-is baseline on the deployment of IoT sensoring and AI/ML solutions to gather and elaborate real-time data on several elements, such as energy usage, peaks, sources, and performances, and (ii) to set up a map of such current solutions. Apply ML techniques to operate data centres more efficiently, which will contribute towards a more efficient and adaptive framework to better understand data centre dynamics and optimise efficiency. Exploit historical data (e.g. temperatures, power, pump speeds) and the PUE (Power Usage Effectiveness) to predict future temperature and pressure of the data centre and recommend the use of certain power supplies according to specific patterns. |
| *Mid-term* | Develop AI/ML standards to integrate in standard guidelines like the Code of Conduct for Energy Efficiency in Data Centres. Progress with standards such as ISO/IEC 23053:2022 to establish an AI and ML framework focused on data centre scenarios. |

## 3.5. Deployment Priority: Data Centre Metrics

#### Key drivers

Data centres have a set of metrics that help to set the benchmark for their success in several areas, including efficiency, sustainability, and density (performance per watt [78]). In this context, Power Usage Effectiveness (PUE) has been widely employed in the research, development, and evaluation of data centres as one of the most important metrics to measure system performance and efficiency. This metric is attractive due to its simplicity. However, conventional cooling has specific limits and data centre owners and operators look towards carbon neutrality or even negativity. Thus, PUE starts to lose its value as a metric. As facilities have become more efficient (PUE of 1.1 and less are commonplace), measuring improvements with PUE becomes harder and gains become increasingly incremental and one-dimensional. In addition to PUE indicators, w other green indicators from the source of the power supply need to be considered, such as water and carbon efficiency, as more comprehensive indicators.

Water Usage Effectiveness (WUE) is an indicator defined as the ratio between the use of water in a data centre system (water loops, adiabatic towers, humidification, water-driven energy production, etc.) and the energy consumption of the IT components. The water needed to produce the energy that powers the data centre is a different aspect to consider. Estimations are that far more water is used for power generation than for IT cooling. Carbon Usage Effectiveness (CUE) aims to measure its sustainability by means of pollutant emissions and it is defined as the relation between the CO2

emissions produced by the data centre and the energy consumption of the IT equipment. Carbon Dioxide Emission Factor (CEF) specifies the CO2 factor of the electrical power.

This value can be dependent on the respective mix of electrical power sources (coal, nuclear, gas, wind, green hydrogen, solar, etc.). Therefore, in an environmentally ideal scenario where a data centre is designed to work with 100% renewable electricity, CUE values theoretically are equal to "0". Based on the above, in addition to PUE, a more holistic approach is required that includes metrics across a range of categories including energy, GHG emissions, water, waste, land, and biodiversity as presented in the following table. Recent frameworks exist [79], designed to help data centre companies to report on their environmental impact and assess their progress towards sustainability through the aforementioned metrics.

| Metric Categories | Key Metrics | Units |
|---|---|---|
| **Energy** | Total energy consumption | kWh |
| | Power usage effectiveness (PUE) | Ratio |
| | Total renewable energy consumption | kWh |
| | Renewable energy factor (REF) | Ratio |
| | Energy Reuse Factor (ERF) | Ratio |
| **GHG emissions** | GHG emissions: (Scope 1) | mtCO2e |
| | Location-based GHG emissions: (Scope 2) | mtCO2e |
| | Market-based GHG emissions: (Scope 2) | mtCO2e |
| | GHG emissions: (Scope 3) | mtCO2e |
| | Location-based carbon intensity (Scope 1+ Scope 2) | mtCO2e/kWh |
| | Market-based carbon intensity (Scope 1+ Scope 2) | mtCO2e/kWh |
| | Carbon usage effectiveness (CUE) | mtCO2e/kWh |
| | Total carbon offsets | mtCO2e |
| **Water** | Total site water usage | $m^3$ |
| | Total source energy water usage | $m^3$ |
| | Water usage effectiveness (WUE) | $m^3$/kWh |
| | Total water use in supply chain | $m^3$ |
| **Waste** | Total waste generated | tons |
| | Waste landfilled | tons |
| | Waste diverted | tons |
| | Waste diversion rate | Ratio |
| **Land & biodiversity** | Mean species abundance (MSA) | MSA/$km^2$ |
| | Euthrofication freshwater | kPEq |
| | Acidification | Mol H+ eq |

*Table 2: 22 example key metrics for reporting environmental sustainability*

### Dependencies

In order to capture and enrich data centre metrics properly, data centre operators, and also component manufacturers, should be encouraged to make this data available via sensors or calculation based on Lice Cycle Analysis (LCA). This is especially true for "new" metrics [80] . Synergy effects exist with *1.1. Technology Priority: Representation in Open Standards, Relation to Norms &* Standards*, 5.1. Technology Priority: Open Standards for Cloud Infrastructure* Services*, and 6.4. Technology Priority: Energy Optimisation and Resource* Conservation.

### Relevant use cases / application domains

For what concerns use cases, data centre measurements are an underlying concern relevant for all use cases listed in the roadmap. Representative ones are listed below:

The *edge-to-cloud continuum / infrastructure* use case highlights several new challenges compared to standard distributed computing systems because of the heterogeneous computing environments, the heterogeneous and dynamic network environments, the node mobility, and the limited power capacity.

The *cross-industry decarbonisation data platforms* use case is relevant in terms of improving the visibility and control of the greenhouse gas (GHG) emissions. Data platforms and data spaces will provide multiple industries with new services to reduce their emissions in line with increasing societal and regulatory requirements. Moreover, the combination of financial, performance, and emissions data is of major importance to ensure appropriate privacy and security.

### *Recommendations*

| | |
|---|---|
| *Short-term* | Select which environmental sustainability metrics a data centre business should track to help drive improvements and compliance, according to the maturity stage of the company and the recommended frameworks / standards. Specify the required monitoring and reporting sustainability targets and metrics. |
| *Mid-term* | Certify the compliance of a set of metrics according to requirements and sustainability frameworks. Perform benchmarking and performance comparison of appropriate metrics to improve, prioritise, and progress over time. Data centre providers are highly encouraged to deliver all relevant KPIs to customers in order to allow them to calculate the end to end environmental impact of their service using data centres (transparency of data). |

# SECTION 4: CYBERSECURITY

The cybersecurity landscape is constantly evolving and cybercrime, besides being among the fastest-growing form of crime worldwide, are also growing in scale, cost and sophistication. This mean that the ability to protect your digital infrastructure and services is a challenge for any organisation regarding technology as well as skills.

This is why many organisations choose established Cloud Service Providers (CSP) that have proven capacity to protect your services 24/7 and the resources to invest in certifications and secure processes.

One concern, compared to traditional on-premises environments, is the shared responsibility model or the supply chain security: some providers are responsible for securing the infrastructure, systems and services, other providers are responsible for connected devices and other connected products, while the customers are responsible for securing their own data and applications.

Another concern is the increased attack surface as more sensitive data is stored and processed in centralised computing environments [82]. This has led to an increase in targeted attacks, such as ransomware and phishing, as well as the use of cloud-native technologies for malicious purposes.

To address these challenges, organisations must adopt a comprehensive security strategy that includes measures such as encryption, identity and access management, and incident response planning [83]. It is important to be aware of the new European Cybersecurity Certification Scheme for both products (EUCC) Cloud Services (EUCS) and for 5G and also compliance standards related to the Cloud Computing (e.g. ISO 27001, SOC 2, PCI-DSS etc.) and ensure the Cloud Service Provider (CSP) is providing the level of security that meets the demand and EU regulations. The focus on human interaction in the domain of cybersecurity is an acknowledgement that humans need security in the digital world. While cloud technology is an enabler and a necessity in several application domains, one aspect of cybersecurity in cloud computing is the level of perceived security and trustworthiness. Despite the evident benefits of cloud and edge computing, its adoption is still limited partially because of what EU customers and industries perceive to be a lack of security and transparency in applied technologies. Cloud Service Providers usually rely on security certifications as a means to improve transparency and trustworthiness. However European CSPs still face multiple challenges for certifying their services, such as the fragmentation in the certification market, the lack of mutual recognition, the feasibility of continuous certification, and the working (technology-based) trust-mechanisms.

# Focus area: Cutting-edge Approaches and Technology Solutions

## 4.1. Technology Priority: EU innovative Data Encryption Technologies including Quantum-safe & Privacy-enhancing Encryptions

### Key drivers

In the edge-to-cloud continuum, data is flowing through and to many different environments controlled by entities that cannot be trusted with sensitive content, hence it is very important to utilise robust encryption capabilities for security and sovereignty purposes. Many encryption mechanisms used today are not quantum safe and the data they protect can already be targeted with a "steal now, decrypt later" strategy. Privacy-Enhancing Cryptography (PEC) seems promising but is only at an early stage with very few applications. These innovative encryption technologies are just emerging and not yet available for global usage. Therefore, Europe needs to foster the development of these technologies by European companies in a sovereign way. There is already a strong European ecosystem in the cryptography field. If Europe clearly defines the needs in terms of PEC, quantum safe encryption, and encryption in harsh conditions, this ecosystem should be able to deliver them. Europe should also make sure the market demand is there by imposing these encryption technologies wherever they are needed to protect EU citizens' and companies' sensitive data.

Additionally, Europe needs to develop innovative encryption technologies that will allow organisations to maintain full control over the security and protection of their data in the cloud, the data transfer from on-premises or cloud infrastructures, as well as cyber-protection for AI applications and SaaS solutions. These include the advanced development of trusted encryption in harsh industrial environmental conditions (e.g. high vibration, temperature, pressure, etc.). They also encompass PEC solutions providing the ability to maintain data in a continuous encrypted state in order to exploit the data without decrypting, such as secure multi-party computation and confidential computing. Moreover, quantum safe encryption technologies should be accelerated to prepare for the quantum cybercrime era, with, for instance, the development of a quantum random number generator using quantum mechanical properties for unpredictable and highly secured encryption keys. Such technologies are critical to European technological sovereignty. Europe could become a global leader in these technologies by leveraging existing ecosystems of partners, intensive R&D activity, and ongoing initiatives like the Quantum Flagship.

### Dependencies

The main dependency of the current priority is to be identified in the scope of *9.8. Technology Priority:* Edge-to-Cloud Blockchain Services, but also in the focus areas of Section 3, as security has to go hand-in-hand with advanced solutions, while addressing relevant issues and considerations.

### Relevant use cases / application domains

Cybersecurity is a relevant topic and also an enabler (in light of trust mechanisms) for all use cases listed in the roadmap. A special representative use case is listed below:

The *cross-industry decarbonisation data platforms* use case is strongly impacted by the need to build trust in technology and application through the development of cybersecurity standards, which enable the secure and transparent exchange of data while maintaining the sovereignty of one's data.

### *Recommendations*

| | |
|---|---|
| *Short-term* | Define a roadmap of availability for PEC, quantum safe encryption, and encryption in harsh conditions, to be delivered by the European ecosystem in the cryptography field, in order to ensure the delivery of European encryption technologies to protect EU citizens' and companies' sensitive data. Fund this roadmap through existing or new programs. |
| *Mid-term* | Publish regulations and certification schemes to require the use of these encryption technologies wherever it is deemed necessary (to protect EU citizens' and companies' sensitive data). |

## 4.2. Technology Priority: Reliable, High-performance, Zero-trust Identity Management

### Key drivers

In the current context of a global adoption of a zero-trust approach to cope with the scattering of IT resources in the edge-to-cloud continuum, Identity and Access Management (IAM) solutions are becoming paramount to security and sovereignty. But as of today, the IAM market is dominated by non-EU solutions and providers. There is a lack of European IAM solution vendors able to compete with worldwide leaders. European vendors are often reduced to niche players in their national market. To overcome this situation, massive investments would be needed to: (i) reach and keep up with the pace of innovation of worldwide leaders, and (ii) target the whole EU market from the beginning.

Moreover, Europe needs to develop a reliable, high-performance, zero-trust identity management solution that restricts connections to those between authorized devices and users by means of an authorized application, and which includes security features to protect against human error. Artificial intelligence (AI) should also be incorporated into this solution both to detect user misbehaviour and to facilitate security reviews, approvals, re-certifications, and re-conciliations of rights over applications. AI can also be exploited to detect threats or facilitate users' and administrators' tasks.

### Dependencies

A dependency of this priority as a pre-requisite can be identified in the scope of *10.2. Technology Priority: Data Spaces and* Networks and in the focus area of advanced solutions - *Focus area: Advanced applications*. Both areas need specific, advanced trust-based identity management solutions to be applicable/ready for further development.

### Relevant use cases / application domains

Cybersecurity is a relevant topic and also an enabler (in the light of trust mechanisms) for all use cases listed in the roadmap. A special representative use case is listed below:

The *cross-industry decarbonisation data platforms* use case is strongly impacted by the need to build trust in technology and application through the development of cybersecurity standards, which enable the secure and transparent exchange of data while maintaining the sovereignty of one's data.

### *Recommendations*

| | |
|---|---|
| *Short-term* | Support European IAM vendors and technology providers (2 or 3 vendors / providers), to emerge at the level of worldwide leaders. The proposed support refers to funding through existing or new programs. |
| *Mid-term* | Deliver regulations and certification schemes to require EU solutions for critical activities in Member States (homogeneously in all of them to open the whole EU market to these EU solutions). |

## 4.3. Technology Priority: Device-Centric Contextual Risk Classification Mapping

### Key drivers

Utilising a risk-based approach is second nature for human beings and nowadays - in the Digital Age - it is a must have. It is implemented and used more and more in the various digital, cyber-physical, and cyber-markets and domains where connectivity, inter-connectivity or even hyper-connectivity play a role. It is also the current and well-known approach for every EU Digital Decade 2030 policy initiative and instrument. Each situation and context creates different risks. These have different risk levels that ethically, socially, or otherwise justify different risk mitigation measures and appropriate levels of accountability. Risk classification, based on context, is therefore an essential starting point to identifying and thereafter mitigating cyber-threats, including sovereignty and cybersecurity issues, and detrimental consequences. However, where should any stakeholder start with identifying what risk means and classifying the risk according to context? And how should such stakeholder do that throughout the entire life cycle? Currently, these are generally not done or properly or consistently considered, let alone implemented. Where any market or ecosystem consists of both demand and supply side (upstream, midstream and downstream) but also various

kinds of users, society, policy makers, supervisors and other stakeholders, each of these stakeholders will have different perspectives.

In this context there is a need for each stakeholder to understand that risk is not a four-letter word. Risk is the dynamic equation of the probability of occurrence or event, times the potential adverse impact, within a particular context and its periphery (both the cyber, cyber-physical and physical domains). As risk is dynamic, changes over time, stakeholders need to have a dynamic risk mapping methodology to do high-level quality risk classification. Risk classification, based on context, therefore is an essential starting point to identifying and thereafter mitigating cyber and related threats.

Being able to: (i) address threats and other challenges, (ii) build, achieve and sustain digital sovereignty, and (iii) prepare for detrimental scenarios, one needs to know and be able to explain to others what risks being addressed and what to verify and assure. This is also the entry point towards layered, multi-layered and holistic, life cycle sovereignty, cybersecurity, and resilience, said otherwise: when to verify and assure. Plotting and mapping what risk to verify and assure is the starting point. The mapping will enable to understand the contextual and dynamic nature of risk throughout the life cycle of (IoT and other) devices, systems, including their subsystems, components, chipsets, operating systems, software, applications, data and other technical and organisational layers, domains and dimensions. Additionally, the combination of the aforementioned layers and domains need to be considered since they highlight the probability and impact in each situation dependent on various technical, organisational, and other dimensions. Mapping the risk and risk classification at connector level should be the first step for every digital system, since the data processing is performed at far edge, edge, or cloud levels. Thereafter, taking in and layering up other risk spectra, such as functionality, data flows, application, intended use, sector, operating system, APIs and so forth caters for identifying the appropriate risk classification, and provides the ability to consider what and how to mitigate the risks.

### Dependencies

Dependencies for this priority relate with almost all other technology priorities of this Roadmap that have a device-centric focus. Among them - for instance - technology priorities of Section 6, Section 8 and Section 9 in particular.

### Relevant use cases / application domains

Cybersecurity is a relevant topic and also an enabler (in the light of trust mechanisms) for all use cases listed in the roadmap. A special representative use case is listed below:

The *cross-industry de-carbonization data platforms* use case is strongly impacted by the need to build trust in technology and application through the development of cybersecurity standards, which enable the secure and transparent exchange of data while maintaining the sovereignty of one's data.

### *Recommendations*

| | |
|---|---|
| *Short-term* | Provide an (inter or hyper) connected device-centric risk classification spectra mapping tackling markets or ecosystems that consist of demand and supply side but which also tackles users, society, policy makers and other stakeholders. Enable a common understanding of risk classifications and increase trust for manufacturers, procurement departments, customers, and policy makers through the proposed risk spectra mapping. |

## 4.4. Deployment Priority: EU automated Security Operation Centres (SOC) for Faster Detection & Response to Cyber-attacks from Cloud to Edge

#### Key drivers

The continuous trend towards a high volume of simultaneous or AI-based cyberattacks targeting critical digital infrastructures cannot be countered with humans' actions only. Therefore, more and more providers of SOC technologies leverage AI and automation to allow them to deliver Managed Detection and Response services. This market is today dominated by non-EU technology providers offering SaaS solutions. Considering the sensitivity of the data flowing into these solutions, this is problematic for the sovereignty of EU organisations. European SOC technology providers able to compete with worldwide leaders are absent. European vendors are often reduced to niche players in their national market. To overcome this situation, massive investments would be needed to: (i) reach and keep up with the pace of innovation of worldwide leaders, and (ii) target the whole EU market from the start.

An additional main key driver is the centralised architecture of today's SOC technologies, which is not well suited to the edge-to-cloud continuum. A decentralised architecture where detection, analysis, and response features are available directly at the edge, would be better adapted. Of course, some central "brain" would still be needed to coordinate all the edges and detect threats impacting the whole environment.

Furthermore, Europe needs to develop SOC with further integration of machine learning and AI-assisted automation technologies in security operations to improve threat anticipation (i.e. access, data privacy, login, and certification), detection (i.e. data analytics and tracing), and response (i.e. incident and problem management). Improvement of AI-based security analytics supported by automation in areas such as policy/compliance as well as forensic and incident response are also key to anticipating attacks or to mitigating them. Such technologies include deep learning for cybersecurity, such as algorithm for deep behavioural profiling and anomaly detection. Moreover, in the edge-to-cloud continuum, these technologies should also deliver edge security analytics in terms of detection, analysis, and response features available directly at the edge, under the coordination of a central "brain". This will also contribute to reducing the flow of data from edge to cloud, hence reducing the carbon footprint.

### Dependencies

The identified dependencies are in *6.3. Deployment Priority: Edge Data Centre Security and* Accessibility as a prerequisite to aim for advanced security in data centres; in *5.1. Technology Priority: Open Standards for Cloud Infrastructure* Services for interconnectivity on security topics (making threat detection possible) and in *9.7. Technology Priority: Edge-to-Cloud Data* Services.

### Relevant use cases / application domains

Cybersecurity is a relevant topic and also an enabler (in the light of trust mechanisms) for all use cases listed in the roadmap. A special representative use case is listed below:

The *cross-industry decarbonisation data platforms* use case is strongly impacted by the need to build trust in technology and application through the development of cybersecurity standards, which enable the secure and transparent exchange of data while maintaining the sovereignty of one's data.

### *Recommendations*

| | |
|---|---|
| *Short-term* | Support European SOC vendors and technology providers (2 or 3 vendors / providers), to emerge at the level of worldwide leaders. The proposed support refers to funding through existing or new programs and can be of different natures (see ENISA's ad-hoc working group on "Security Operation Centres" [84]). |
| *Mid-term* | Deliver regulations and certification schemes to require EU solutions for critical activities in Member States (homogeneously in all of them to open the whole EU market to these EU solutions). Standardise the mechanisms and APIs of ICT components to allow efficient automation of threat responses. |

# Focus area: Setting the Scene and Fostering Standardisation

## 4.5. Technology Priority: Landscaping Existing EU Projects' Cybersecurity Deliverables

### Key drivers

Massive amounts of EU resources and funds from Horizon 2020 and other programs have been allocated to projects focusing on / addressing cybersecurity and related topics regarding digital sovereignty. However, there is no clarity, actionable overview, or other readily available oversight and insights into whether, and to what extent, project results are concrete, useful, viable, effective, and sustainable to add to the building, achieving, and sustainability of European digital sovereignty, in particular from the perspectives of cybersecurity, cyber-physical security, and

related security domains and dimensions. For instance, what are the various TRLs (Technology Readiness Levels) of the cybersecurity capabilities researched, developed, and furthered, and what requires improvement, optimisation, updating, preparing for implementation and deployment, and sharing with EU stakeholders so that these can contribute to addressing the real-life cyber threat landscape.

Having a clear, practical, and useful landscape of the EU programs and related projects' cybersecurity deliverables and other results is required. It can provide oversight into what has already been done, where it can be usefully deployed and further developed, and what is still missing. Just mapping those geographically is not enough; the various deliverables and results – and, where available, post-project dissemination activities – will need to be vetted at merit. The other main objective is to identify synergies, gaps, and improvements, and use these for consideration for (further) investments. Where possible, one can also consider inviting, assessing, and where appropriate up taking the deliverables and results from similar cybersecurity-related projects of Member States or regions as well.

### Dependencies

The basics to start the work are at hand in databases like CORDIS. A dependency with *the 2.5.* Technology Priority: Make EU Regulations fit for a Digital Sovereign Europe exists as it stresses the need to make EU regulation fit for the digital sovereign Europe, for which the cybersecurity landscape plays a big role.

### Relevant use cases / application domains

Cybersecurity is a relevant topic and also an enabler (in the light of trust mechanisms) for all use cases listed in the roadmap. A special representative use case is listed below:

The *cross-industry decarbonisation data platforms* use case is strongly impacted by the need to build trust in technology and application through the development of cybersecurity standards, which enable the secure and transparent exchange of data while maintaining the sovereignty of one's data.

## *Recommendations*

| | |
|---|---|
| *Short-term* | Identification of the EU programs and related projects' cybersecurity deliverables and results that can contribute to the building, achieving, and sustainability of European digital sovereignty from cybersecurity perspectives. Structured visualization in identified cybersecurity domains and dimensions of cybersecurity research activities, innovation activities, and related products, systems, and services of European organisations that are active in the cybersecurity domain. |
| *Mid-term* | Identification of synergies, gaps, and improvements to facilitate the building, achieving, and sustainability of European digital sovereignty from cybersecurity |

| | |
|---|---|
| | perspectives. For such vetting purposes, for instance, the various angles of the evaluation components and queries of the European Innovation Council (EIC) and related lessons learned could be considered and optimised. |

## 4.6. Technology Priority: Member State NIS2 Directive Comfort & Capability Building

### Key drivers

The Network and Information (NIS) Directive (both the previous and the current NIS2) aims to enhance the readiness in particular sectors responsible for critical infrastructures, vital systems, and essential services. Compared to other critical infrastructure regulations outside the EU, the NIS2 Directive is the current state of the art. However, currently not all sectors mentioned in the NIS2 Directive are covered by each Member State. The levels of implementation differ substantially, therefore reducing the operational effectiveness of the response to large-scale cybersecurity incidents or zero-day vulnerabilities. It also reduces the effectiveness of the strategic aims of the NIS2 Directive and, subsequently, the chances of success when it comes to building and sustaining digital sovereignty within the EU. Identifying and addressing each reason for the difference in levels of implementation is the only way to support building, achieving, and sustaining digital sovereignty of European (Member States and related) critical infrastructures, vital systems, and essential services. The differences in levels of implementation represent a substantial vulnerability, as systems are generally interdependent, influence each other, and can infect or negatively affect each other. The reasons for differences could include the lack of expertise to implement in a particular sector, potential hurdles or other preconditions, or the lack of resources, funds, or other capabilities.

### Relevant use cases / application domains

Cybersecurity is a relevant topic and also an enabler (in the light of trust mechanisms) for all use cases listed in the roadmap. A special representative use case is listed below:

The *cross-industry decarbonisation data platforms* use case is strongly impacted by the need to build trust in technologies / applications through the development of cybersecurity standards, enabling the secure and transparent exchange of data while maintaining the sovereignty of one's data.

### *Recommendations*

| | |
|---|---|
| *Short-term* | Foster and encourage harmonisation in the adoption and implementation of the same or sufficient level of sector coverage to assist in mitigating vulnerabilities in critical infrastructures, vital systems, and essential services which are not bound by physical borders. Progress on a sector-by-sector basis, where the sector that adds |

| | |
|---|---|
| | the most appreciation to the respective Member State is addressed. It may also be the sector that brings synergies to the resilience of interlinked sectors in a Member State or even augments resilience to similar sectors in other Member States. |

## 4.7. Deployment Priority: EU Standardisation Efforts for Stating Cybersecurity Requirements

The current EUCS draft version (December 2021) requests continuous and automated certification / compliance for the security level "standard high". However, it does not state – yet – how to technically achieve that and if this is applicable for all requirement categories. Several European research projects tackle this issue and provide solutions and feasible approaches. The formal exchange for "standard high" will need a standardised, machine-readable notation to state the requirements of the EUCS for this certification level and its control sets. ETSI's TC-CYBER Critical Security Controls, mappings to Canadian Standards Association (CSA), Groupe Speciale Mobile Association (GSMA), National Institute of Standards and Technology (NIST) 800-53, and 27001:2022 controls, and Open Security Controls Assessment Language (OSCAL) expression could be of considerable utility for implementing the EUCS.

It seems beneficial to use an already growing standard NIST OSCAL to write standards and control sets. The OSCAL platform continues to evolve and already engages a wide array of parties within its community. Even though OSCAL is emerging from the US, Europe's role through ETSI and ENISA would be as a global leader in facilitating implementable ICT security capabilities among their enormous array of public and private sector members.

### *Recommendations*

| | |
|---|---|
| *Short-term* | Develop a guidance of how to use OSCAL, moving forward with translating EUCS controls into OSCAL notation, and facilitating use and interoperability by others. This will encourage EU-use of open control specifications for meeting directive requirements and will provide the ground as an international format (through OSCAL information) that can be referenced to meet normative requirements. |
| *Mid-term* | Facilitate creation and availability of additional OSCAL serializations for specialised environments and interoperability testing. Place ETSI / ENISA at an international leadership forefront in getting OSCAL widely-implemented. |

## 4.8. Deployment Priority: Supply Chain – Driver Certification for Hardware Devices

Firmware / drivers / Baseboard Management Controllers (BMCs) / microcode represent a significant threat vector for cloud and edge appliances, server, and associated infrastructure. This is typically the first code executed on a device when it powers on. If this code is compromised the entire system can and should no longer be trusted as a secure device. This firmware can be compromised through malicious attacks or unintentionally. Users of a device must always be able to fully trust the physical device to run the intended and secure firmware. This represents the most fundamental root of trust. The OCP Security working project published a paper on common security threats and undertook extensive work to tackle these threats together with the OCP solution providers.

### *Recommendations*

| | |
|---|---|
| *Short-term* | Create security among firmware developers. Define a secure European Open Reference Architecture to promote a Secure-by-Design mindset and offer a foundational Root of Trust architecture by involving the firmware developers in the early stages of the design and architectural work. |

# SECTION 5: INTEROPERABILITY AND MULTI-PROVIDER SERVICES

The European providers' landscape is fragmented into a number of application, service and infrastructure providers. For industrial and research usages it has become usual to deploy applications across several European providers. This showcases the fragmented landscape of providers across geographies, edge cloud scenarios, and incompatible commercial legal frameworks. The lack of interoperability in the European multi-provider scenario limits the ability of users to deploy applications, limits the choice to switch between suppliers, and limits the providers' ability to (virtually) scale their offerings. Industry requires global solutions and, hence, interoperability cannot be limited to European providers. It is therefore necessary to provide technical specifications and standards to allow interoperability for the European multi-provider scenario as well as with global players.

The development of a sovereign European cloud, with the participation of European companies, the European Union, and Member States, will result in a more uniform European edge-to-cloud continuum landscape. Such a cloud could then support a series of basic services that individual providers would be able to expand and adapt following rules of comparability.

Federated cloud refers to cloud infrastructure, platforms, and software services which are geographically distributed and/or supplied by different providers. It can include the federation of complete cloud data centre services or/and cloud edge services or/and a composition of various layers of the stack (IaaS/PaaS/SaaS). The federated services should allow the user to manage them from a single point (i.e. single pane of glass). In a distributed system, services like interoperability, security, and interconnection are of great importance. To offer a variety of services across a certain footprint, the set of federated providers providing that coverage must provide compatible and interoperable services. Service access, compliance, and quality must also be based on common standards with a strong focus on user requirements and usability.

## Focus area: Standards for a Uniform Abstraction Layer

### 5.1. Technology Priority: Open Standards for Cloud Infrastructure Services

#### Key drivers

To enable interoperability and portability, commonly agreed (standardised) and open APIs together with open source reference implementations are crucial. Besides the specification of those open APIs, this also comprises the provisioning of open documentation and open reference implementations of client libraries for those open APIs. The implementation of such open

standards will enable a high level of interoperability, portability, reversibility, and interconnectivity, as well as to provide service diversity.

However, the development and implementation of standards requires time. Europe is putting efforts into having the first sets of standards but cannot wait to complete the standardisation work to start its implementation. Thus, in the short term some compromise regarding the standardisation approach must be agreed upon in order to advance in the development and the deployment of the edge-to-cloud continuum. The latter should initially cover a basic set of infrastructure services, such as compute, storage, network, and cloud native services, like container and container management, keeping in mind that the standards will evolve as technology progresses. Further to this, with time it will be extended across the complete edge-to-cloud continuum to achieve a sovereign European cloud.

Based on appropriate European or international standards, the development of compatible services and offers across providers is necessary to guarantee a high degree of interoperability, portability, and reversibility of infrastructure and data. Digitalisation of cross-domain services relies on interoperability – also supporting the possibility of portability. While both interoperability and portability should be defined as general objectives and key requirements to be met under a European cloud-edge ecosystem, specific solutions following the needs of different verticals are necessary and may be provided by different vendors.

Cloud interoperability has been covered in the research literature [85] and has been identified as one of the main challenges [86] to be tackled for the future of Cloud Computing. Important lessons can be learned from previous efforts in the Grid Computing community, where the Open Grid Forum (OGF) defined standards like GridFTP [87], OGSA BES (Basic Execution Service), JSDL (Job Submission Description Language), DRMAA (Distributed Resource Management Application API), and even OCCI (Open Cloud Computing Interface). Meanwhile, the OGF's Grid Interoperation Now (GIN) community group coordinated interoperation efforts to overcome the lack of standards in some areas.

In the cloud domain, different organisations have been working on standards for cloud interoperability and portability, including Open Grid Forum (OGF), Distributed Management Task Force (DMTF), Storage Networking Industry Association (SNIA), Organisation for the Advancement of Structured Information Standards (OASIS), Institute of Electrical and Electronics Engineers (IEEE) or Internet Engineering Task Force (IETF). The fruits of their effort are that many open standards for cloud platform management are now available, including OGF Open Cloud Computing Interface (OCCI), SNIA Cloud Data Management Interface (CDMI), DMTF Open Virtualization Format (OVF), DMTF Cloud Infrastructure Managements Interface (CIMI), DMTF Cloud Auditing Data Federation (CADF), OASIS Cloud Application Management Protocol (CAMP), OASIS Cloud Authorization (CloudAuthZ), and OASIS Topology and Orchestration Specification for Cloud Applications (TOSCA). Other organisations have provided guidelines for cloud interoperability and portability,

like the Cloud Standards Customer Council (CSCC) [88], the European Telecommunications Standards Institute (ETSI) [89], or the National Institute of Standards and Technology (NIST) [90].

Since 2019, the telecommunication operator community has been working on the standardisation of edge computing services for applications requiring a footprint spanning across several geographies and providers, following the same principles of service universality, interoperability, and portability that the Mobile industry has applied to voice, messaging, and internet access services. In March 2020, GSMA launched the Operator Platform Group (OPG) [91], a technical group specifying requirements, architecture and open APIs to expose "as a Service" edge computing and other cloud and telecommunication services like NaaS. At the same time, GSMA created the Telco Edge Cloud Forum [92] to trial OPG concepts showing its applicability in different edge use cases and testing the interconnection of different edge providers, demonstrating how this could enable a one-stop-shop approach that simplifies the use of edge computing services across different markets for customers. In February 2022, several telecom operators, technology, and cloud providers launched an open source project at the Linux Foundation, CAMARA [93], in collaboration with the GSMA, that aims to develop open source standard APIs that provide access to operator capabilities regardless of the networks customers are in. One of the working groups is dedicated to edge cloud services. Additionally, in November 2022, several telecom operators and network function vendors in Europe, launched an open source project at the Linux Foundation Europe, SYLVA [94], that aims to develop open source standard telecommunications reference stack to host operator network function and be ready to host B2B application. More recently (in February 2023), GSMA announced that a set of 21 operators had signed the Open Gateway [33] agreement to deliver standard API-based services, including NaaS and Edge, across their combined footprint.

Either the establishment of an agile standardisation body or a European de facto standard is necessary to support innovation and fast implementation, the latter being the most appropriate way to make the solution competitive.

### Dependencies

*1.2. Technology Priority: Open Specifications & Open Source Reference* Implementations*:* Open specifications and the open source software communities are attractive for solving heterogeneous multi-vendor challenges.2.6. Technology Priority: Support Distributed & Interoperable Architectures*:* The support will allow innovation to emerge and the provision of different services of a higher quality through the use of a more distributed and interoperable cloud and edge infrastructure.

*8.1. Technology Priority: Establish an Open Hardware* Ecosystem*:* There is a need to standardise the hardware since it is not possible to build special hardware for each edge site.

### *Recommendations*

| | |
|---|---|
| *Short-term* | Establish standards for a basic set of infrastructure services and provision of open source reference implementations, leveraging ongoing efforts towards standardisation and open source. Assess and support the existing initiatives (e.g. from the telecommunications sector) to contribute to the success of the recommendation. |
| *Mid-term* | Establish and foster existing standards for the complete edge-to-cloud continuum, including vertical sectors. Continued support for existing initiatives that support this goal with an appropriate mandate from the public sector. |
| *Long-term* | Establish or empower a European standardisation body able to foster norms, provide recommendations and guidelines, and certify service providers and tools regarding standards adoption and compliance. |

## 5.2. Technology Priority: Uniform Abstraction Layer for Multi-provider Portability

#### Key drivers

An abstraction layer is required to enable efficient deployment and uninstalling of all services provided within the edge-to-cloud continuum. Sufficient progress has been made in the mobile network architecture realm, but the need is to move beyond this and include all computing capabilities across all types of networks in order to provide seamless and quickly deployable third-party services.

The abstraction layer should offer an automated service discovery module to scan networks and identify resources, easing their migration from one cloud to another. It should also offer transparent service and pricing discovery tools to track used services and their costs, and to provide a clear overview of cloud usage across the different providers. The basic elements for the *Uniform Abstraction Layer* are the following: (i) an *API Portal* to register and maintain API services, (ii) a *reference API Gateway* to secure and route API requests, (iii) a *portal* acting as the user endpoint, collaboration, and documentation space, and (iv) a set of *analytic functions* for reporting and possible monetization. The abstraction layer should be integrated in the EU Federated Cloud Marketplace (please refer to Section 5.3.4) and in the Single Pane of Glass.

The abstraction layer should provide the possibility to manage and deploy resources on different cloud environments, on different cloud providers.

Building European cloud-edge offerings on the basis of open source components, when possible, should be considered to favour appropriation and enforce security. The European cloud-edge offering should create and implement its core infrastructure (such as compute, storage, and

network) following standards for accessibility, scalability, and comparability, and make them available through APIs to be easily integrable and portable from and to other cloud providers' environments.

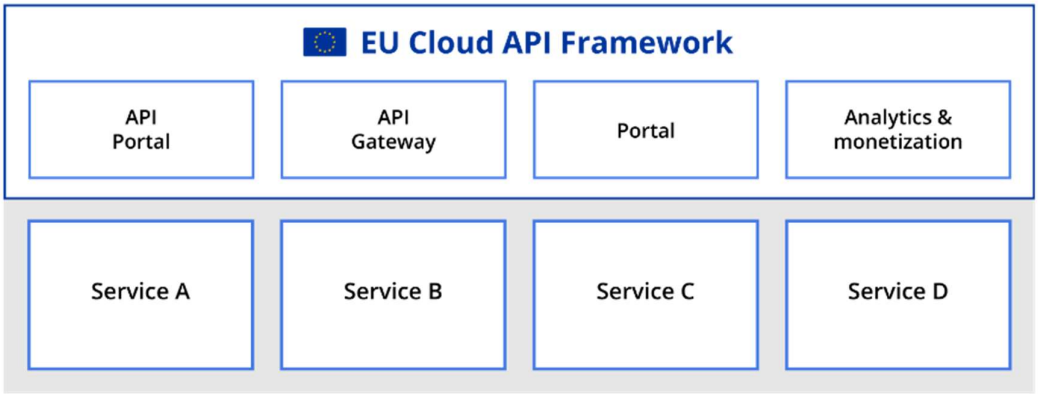



*Figure 10Figure 10: Uniform Abstraction Layer*

The abstraction layer should capitalize on standardised APIs and services to ensure their portability between cloud providers, and offer both northbound APIs and user Interfaces to manage DevOps and basic configurations. As a centric part of a multi-cloud environment, the abstraction layer should be highly secured, with enforced data privacy mechanisms.

### Dependencies

*2.1. Technology Priority: Landscape Sovereignty-enabling* European Digital Capabilities*:* Leverage existing assets and consolidate these towards scalable operations.

*3.1. Technology Priority: Sustainability by* Design*:* It is important to embed such design principles into the development of services from "cradle to grave".3.4. Technology Priority: Use of Digital Technology as AI/ML*:* AI and ML will optimise the distribution of workloads considering environmental and energy efficiency factors.

*4.2. Technology Priority: Reliable, High-performance, Zero-trust Identity* Management*:* Zero-trust adoption to cope with the scattering of resources that we have in the edge-to-cloud continuum.

*Focus area: Innovative Design, Operation:* Today basic building blocks for cloud native applications lack commonly adopted standards which poses a management challenge to design, move, replace, orchestrate, and update distributed edge-cloud nodes.

*7.2. Technology Priority: Control & Orchestration for Edge Connectivity at* Scale*:* Edge applications will require allocation or prioritisation of scarce network resources. Offering these at scale will require automatic, on-demand and as-a-service mechanisms.

*Focus area: Edge-to-Cloud Service Life Cycle Management:* Specify a cloud and edge software stack with standardised and open interfaces, and ultimately ensure their implementation in software offerings.

#### Relevant use cases / application domains

In general, any edge application that is to be delivered over a global or multinational footprint will benefit from a portability-enabling abstraction layer. Representative examples follow.

The users described in the *smart and secure mobility* use case need a uniform abstraction layer so services are not disconnected as they roam across multiple geographies.

The services described in *global freight and people logistics* use case will be obtained from a multitude of providers across diverse geographic locations, thus the need for a uniform abstraction layer.

#### *Recommendations*

| | |
|---|---|
| *Short-term* | Specify and design the Uniform Abstraction Layer with an API portal to register and maintain API services, a reference API Gateway to secure and route API requests, a portal as the user endpoint, the collaboration, and documentation space. Integrate the abstraction layer in the Federated Cloud Marketplace. Assess and support existing candidate tools that could serve as initial implementation. |
| *Mid/long-term* | Improve the Uniform Abstraction Layer with analytic functions for reporting and possible monetization. Integrate the abstraction layer in a multi-cloud-edge control plane. Implement an SDK to provide function libraries for the device applications to contact the edge-cloud platform to request information or trigger actions. Develop enforced data privacy mechanisms and sovereignty. Promote their adoption by IaaS providers. |

# Focus area: Orchestration and Federation of Distributed Edge Cloud

## 5.3. Technology Priority: Multi-provider Meta-Orchestration and Workload Optimisation

#### Key drivers

A Single Pane of Glass should provide the possibility to manage and deploy services on different cloud environments through different cloud providers. Such a tool would enable the selection of the best provider(s) according to different criteria like performance, reliability, cost, energy

efficiency or regulations. Workload could be optimised in several ways, taking advantage of the new emerging paradigm of adaptive hybrid computing or cognitive cloud and edge, orchestrated by artificially intelligent system management engines. This way, several smart mechanisms could be put in place, like anomaly detection, capacity adjustment, or security compliance. Taking full advantage of AI and ML advances, which are now commonplace in the digital and data spaces, will contribute to making the deployment of any kind of service in the edge-to-cloud continuum a commercially viable reality. Section 6 provides a more in-depth view of this subject.

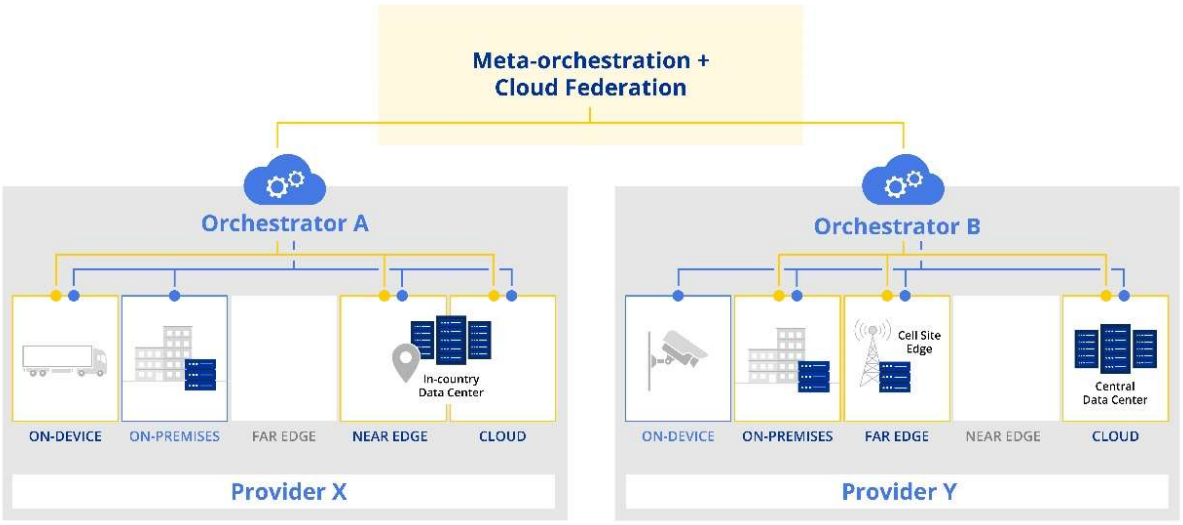



*Figure 11: Meta-orchestration and federation of providers*

It should be noted that the Single Pane of Glass requires a large consensus from all participating organisations.

Dependencies3.4. Technology Priority: Use of Digital Technology as AI/ML*:* Optimise the distribution of workloads considering environmental and energy efficiency factors, developing sustainable solutions to analyse energy consumption.

*4.2. Technology Priority: Reliable, High-performance, Zero-trust Identity* Management*:* Zero-trust adoption to cope with the scattering of resources that we have in the edge-to-cloud continuum.

*6.2. Technology Priority: Advanced Simulation and Prediction Capabilities for* Operation*:* Create tools and techniques for an effective and efficient reduction of carbon footprints to be more sustainable.

*8.6. Technology Priority: Improving Software for Hardware Operation, Management, and* Monitoring*:* There is a need to develop new technologies to handle millions of heterogeneous devices.

### Relevant use cases / application domains

The cross-vendor interoperability and standardised data sharing demanded by the *"next-gen engagement" and human centricity* use case across the edge-to-cloud continuum highlight the need for meta-orchestration and federation of providers.

Mobility as a service and autonomous driving solutions, as highlighted in the *smart and secure mobility* use case, require real-time data exchange between devices, while scalable capacity to run AI models across the edge-to-cloud continuum needs meta-orchestration and workload optimisation.

In the *public safety and disaster relief* use case, the Interoperable safety platform and the required faster data exchange among local services across the EU region requires multi-provider meta-orchestration to simplify coordination and cooperation among services.

### *Recommendations*

| | |
|---|---|
| *Short-term* | Specify and design a framework to serve as the Single Pane of Glass, including management and deployment of resources on different cloud environments through different cloud providers, the selection of the best provider(s) according to different criteria, workload optimisation with adaptive hybrid computing or cognitive cloud and edge. Assess and support candidate open-source components to serve as initial implementation of this tool. |
| *Mid/long-term* | Improve the Single Pane of Glass framework, for example, by taking full advantage of AI and ML to put in place smart mechanisms, like anomaly detection, capacity adjustment, or security compliance. Promote its adoption by end users, either as on-premises deployment or through a SaaS model. Focus and support from the telecommunications and public sectors is critical for the successful implementation and adoption of the framework. |

## 5.4. Technology Priority: Multi-provider Edge Cloud Federation

### Key drivers

Federation is understood as a group of service providers agreeing upon standards of operation so they can work in a collective and decentralised fashion to deliver a set of common services over their combined footprint. Thus, this allows the deployment and seamless operation of a service with a uniform QoS level across the entire edge-to-cloud continuum. With the advent of edge computing and the need to transverse one or more administrative domains to provide the edge-to-cloud continuum in multiple directions, the existing master-slave relationship in current aggregation solutions (as depicted in the left in Figure 12) must be redefined to attain a peer-to-peer relationship in the foreseeable future.

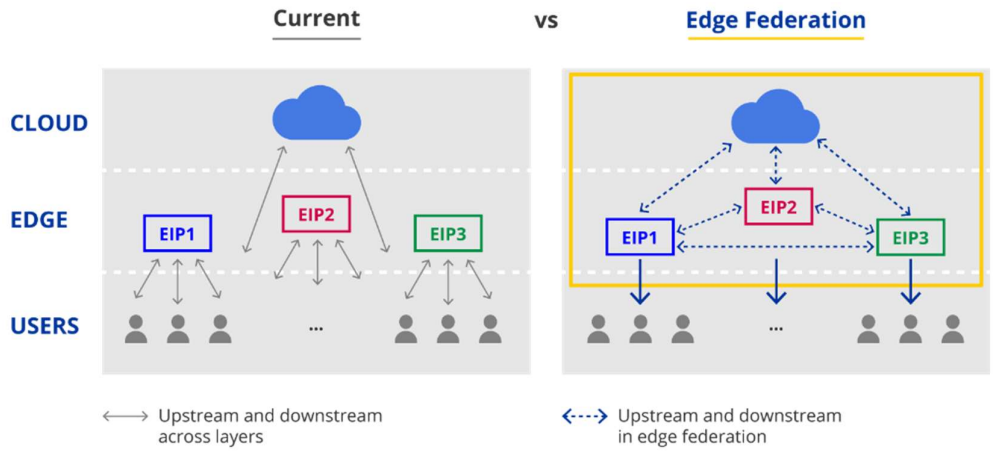



*Figure 12: Edge federation concept*

As far as it is technologically feasible, meta-orchestration and cloud federation should not generate a negative impact to the performance of the edge-to-cloud continuum; the statement sounds obvious but it requires that the meta-orchestration and cloud federation mechanisms be as simple as possible with the least number of interfaces so as not to impose unnecessary overheads.

One of the common points of the architecture of the described NaaS Orchestration frameworks, in Section 7, is the lack of ability to orchestrate network services spanning multiple administrative domains. In next-generation mobile networks, such scenarios are very relevant because these networks are expected to operate in highly heterogeneous environments, not only at the "resource layer" by supporting different access and transport technologies, but also at the "service layer", where some necessary functions to deploy network services (NFV-NSs) can be provided by different organisations, hence requiring service federation capabilities, as further explained in Section 10.

The H2020 project BEACON (2015-2017) enabled the provision and management of cross-site virtual networks for federated cloud infrastructures, to support the automated deployment of applications and services across different clouds and data centres. Furthermore, recently two practical test examples of edge federation mechanisms were delivered: in 2020 the Multi-Operator MEC POC [95] and in early 2022 the Telco Edge Cloud (TEC) Trial – Bridge Alliance Federated Edge Hub and MobiledgeX Interconnection [96]. As a result of this experience, GSMA delivered some technical requirements and specifications in October 2022 for the East-Westbound Interface APIs [154]. Moreover, work has begun on developing the open source implementation of the Federation APIs in GSMA as part of the Operator Platform group activities.

Leading European network operators together with relevant open source software developers should work together in the creation of a platform led by the EU industry capable of solving the key issues described above. In the IPCEI-CIS Project such a proposal already exists and should be given proper support by entities and organisations beyond the ones involved in the project.

### Dependencies

*7.9. Deployment Priority: Coordination of Network Orchestration with Multi-cloud* Orchestration*:* Slice orchestration relies on the multi-cloud orchestration to automatically deploy and scale up and down the network resource capacity.

### Relevant use cases / application domains

Mobility as a service and autonomous driving solutions, as highlighted in the *smart and secure mobility* use case, require real-time data exchange between devices, while scalable capacity to run AI models across the edge-to-cloud continuum needs a multi-provider edge cloud federation.

In *smart city* use cases, multi-provider edge cloud federation is required to optimise resource usage and improve the quality of life by connecting and utilising data from different sectors (e.g. power plant, utilities, infrastructure, health, mobility, etc).

As highlighted in the *digital supply chain* use case, the need for transparency and control of virtual and physical goods and services across the geography in thousands of edge nodes poses the need for multi-provider edge cloud federation.

### *Recommendations*

| | |
|---|---|
| *Short-term* | Support and boost projects and EU initiatives to deploy the cloud-edge infrastructure that will support the multi-provider edge cloud federation. |
| *Mid-term* | Adopt the new edge federation model, transitioning from the existing master-slave relationship in current aggregation solutions to a peer-to-peer relationship between edge locations. Reduce the overheads of meta-orchestration and cloud federation mechanisms and also reduce their complexity in terms of number of interfaces and interactions. Focus and support from the telecommunications and public sectors is critical for the successful implementation and adoption of the edge federation model. |

## 5.5. Deployment Priority: Reference Test Bed for Edge-to-Cloud Continuum Deployment

### Key drivers

The testbed deployment will provide a real-world reference implementation of a European sovereign edge-to-cloud continuum infrastructure as described in Section 10 and the Important Projects of Common European Interest (IPCEI) with a special focus on the Next-Generation Cloud Infrastructure and Services (IPCEI-CIS). Different Task Force areas will come together to show the power of joint development and cooperation across Europe. To enable efficient funding, this reference implementation should be transferred to a productive landscape at a later stage. This

reference implementation can be used as a blueprint for deployment at large scale. The figure illustrates a possible set-up, with two regional data centres, multiple availability zones, including the integration of nodes all the way from near-edge to on-premises infrastructure, seamlessly connected.

The integration of further aspects like sustainability, cybersecurity, data centre, cloud, cloud software, could make it a lighthouse development and showcase the European cloud efforts. The success of the initiative would also demonstrate the European technological leadership. Possible use cases are the operation of systems of the European Union or from the academic world.

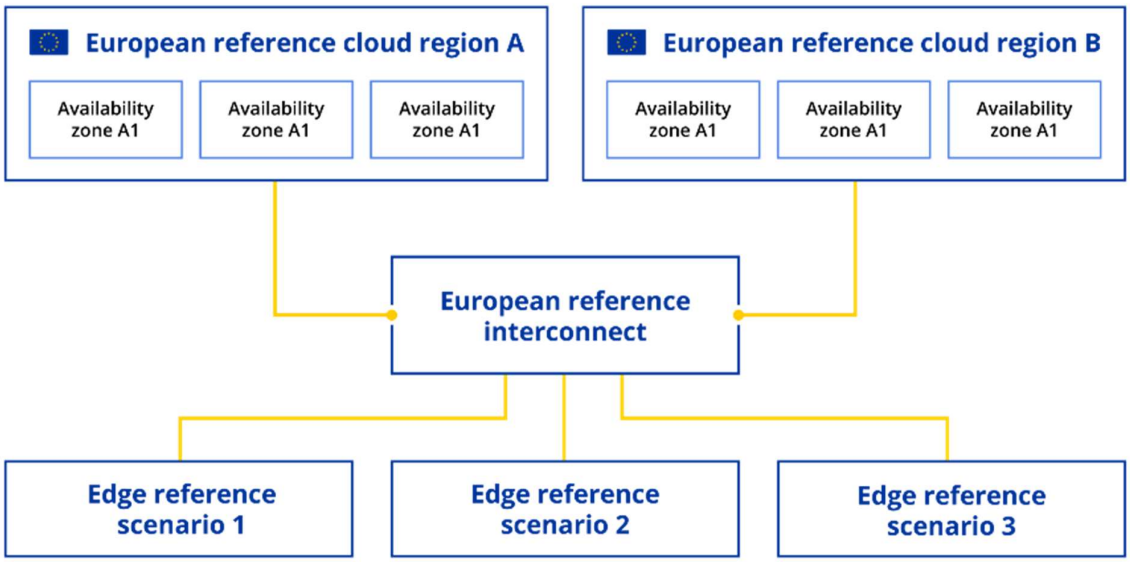



*Figure 13: Deployment test bed reference architecture*

### Dependencies

*Focus area: Standards for a Uniform Abstraction Layer:* Interoperability is a must to foster innovation and collaboration to build the edge-to-cloud continuum, especially for edge applications deployed across a wide geographic scale.

*Focus area: Open specifications and standards, reference implementations, and open* source*:* Identify ways to educate companies to support open source and to understand its innovation model with the opportunities it brings to open up new business areas without compromising their intellectual property. Moreover, define a Europe-wide plan to promote the benefits of open source and the role of innovation around open standards and open source technologies.

### Relevant use cases / application domains

The testbed will allow R&D to overcome several new complicated challenges compared to standard distributed computing systems of the heterogeneous computing environment, heterogeneous and dynamic network environment, node mobility, and limited power capacity. This could be utilised in infrastructure use cases across the edge-to-cloud continuum.

The testbed will allow realistic testing in the domain of the telecommunications industry itself, with a foreseen wide applicability in mobile networks driving cloud edge.

### *Recommendations*

| | |
|---|---|
| *Short-term* | Design a Reference Testbed for edge-to-cloud continuum deployment as described in Section 10. In particular, define the requirements of the necessary central services and the requirements for sites to join the testbed (e.g. implementation of standards or use of the Uniform Abstraction Layer tool). |
| *Mid-term* | Improve the Reference Testbed for edge-to-cloud continuum deployment, fostering joint development and cooperation across Europe and integrating further aspects like sustainability, cybersecurity, data centre, cloud and cloud software. Promote its use by end users and encourage sites to join. |
| *Long-term* | Maintain the Reference Testbed for edge-to-cloud continuum deployment and provide long term support for it. |

## 5.6. Deployment Priority: Federated Cloud Marketplace

#### Key drivers

The marketplace serves as a one-stop shop for cloud-edge applications and infrastructure from all providers that abide by European regulation. It is expected to lower barriers to entry for smaller service providers. Under its most simple format, a European cloud marketplace would aggregate compliant services into an openly accessible, certified catalogue, with a search function allowing users to find solutions that match their criteria. Beyond this information-sharing and match-making capability, the marketplace could also provide brokering features to facilitate transactions between providers and customers.

The marketplace should be built to enable multi-tenancy: the service catalogue and technical foundations would be the same across Europe but would allow different entities to operate the marketplace for different user bases. For example, Member States wishing to have their own marketplace for their national public sector consumption of cloud and services according to a specific framework contract could operate an instance of the marketplace and thereby still access the same service catalogue. A network of connected instances could thereby feed into a meta service catalogue.

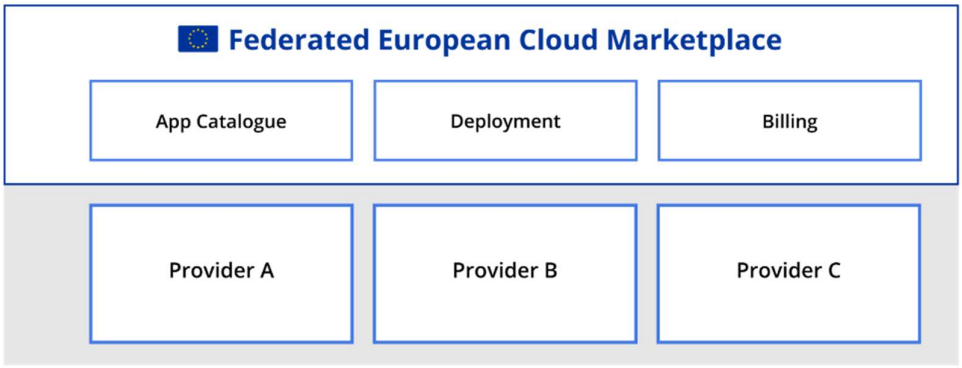



*Figure 14: Federated European cloud marketplace*

### Dependencies

*1.3. Technology Priority: Closer Collaboration between Initiatives and* Associations*:* Avoid "excessive regulation" that may create the preconditions for market fragmentation and instead define a regulatory regime that provides complete harmonisation.

*Focus area: Standards for a Uniform Abstraction Layer:* A major challenge is to coordinate all stakeholders of the different interfaces and APIs and promote the use of alternative standards.

### Relevant use cases / application domains

*AI Federated machine learning* at the edge is a representative application/approach that focuses on training AI models across edge nodes without the need to transfer data to the cloud to preserve privacy and bandwidth, and the federated cloud marketplace is a key enabler.

The ability to make data from physical devices available to an IT system and drive actions back to the physical world with an extensive variety of such devices requires the existence of a federated cloud marketplace to facilitate commonality of applications. The latter could be applied in a use case related to *digital twins - linking Operational Technologies (OT) systems to IT representation*.

### *Recommendations*

| | |
|---|---|
| *Short-term* | Design a Federated Cloud Marketplace as an openly accessible, certified catalogue of applications and infrastructure from all providers who abide by European regulation and who provide information-sharing and match-making capabilities. Assess and support candidate open source tools to serve as initial implementation of this tool. |
| *Mid-term* | Improve the Federated Cloud Marketplace, providing brokering features to facilitate transactions between providers and customers. Promote its use by end users and IaaS providers. |
| *Long-term* | Maintain the Federated Cloud Marketplace and provide long term support for it. |

# SECTION 6: EDGE AND DATA CENTRE INFRASTRUCTURE

Organizations are faced with the challenge of driving digitization forward, meeting sustainability goals and reducing costs at the same time. They are therefore turning their attention to their digital infrastructure, especially the cloud, in order to achieve better cost control implementing new approaches and tailor-made solutions to optimize cloud workloads and services.

Cloud optimization will move from a pure focus on avoiding wasting cloud resources to determining the most efficient way to optimize and allocate cloud resources, particularly the orchestration of distributed hybrid or multi-cloud use cases.

To provide the best possible user and customer experience, organizations are moving cloud applications to the edge. Speed and latency are key attributes to enable a better user and customer experience, the key promises of edge applications and edge infrastructure.

With the traditional cloud approach, the services are centralized in the region of the cloud provider. Edge computing moves compute and storage resources closer to the user and where the applications are provided. This also reduces costs, security risks and energy consumption for data transmission, storage and processing.

It is becoming apparent that the trend is moving away from centralized towards decentralized data centre infrastructure. This requires adequate capabilities to manage the infrastructure associated with the growing number of distributed edge nodes [84] as well as the implementation and adoption of new sustainable data centre designs that take local and regional conditions and regulations into account.

With the rising demand for federated edge infrastructure, cloud infrastructure and service providers will have to collaborate more closely with telecommunication and network providers, utilities and municipalities to establish an integrated and sustainable edge to cloud ecosystem.

This chapter describes two focus areas that deal with the design and operation of data centres to increase efficiency and sustainability. An important factor in enabling this and measuring success is the integration of artificial intelligence, digital twins and building information modelling for data centre infrastructure management and data centre design. Figure 15 provides an overview of the current topics that are being dealt with in the area of data centre design and operation.

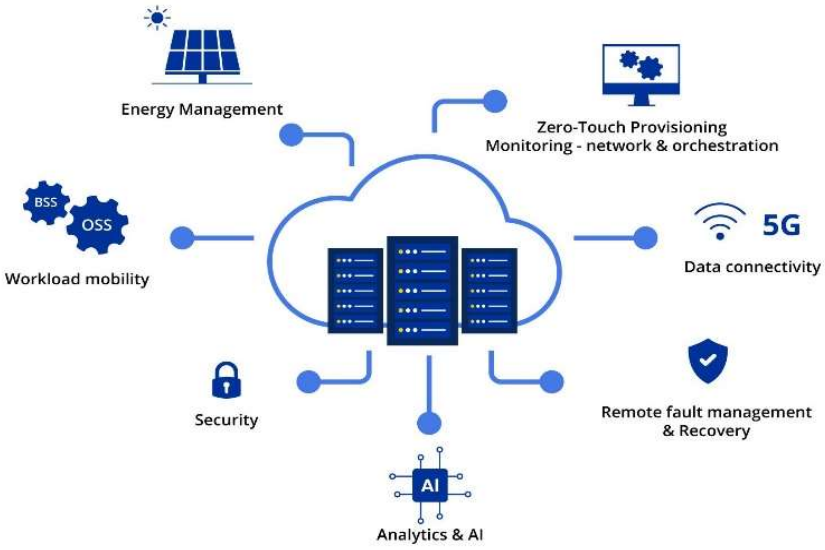



*Figure 15: AI-enabled functionality for edge and data centre infrastructure*

## Focus area: Innovative Design, Operation and Security

Mobile employees and customers consume cloud services on the go. To ensure users have a good experience and to provide them access from anywhere, a flexible and efficient data centre and service operation must be guaranteed at the same time.

Therefore. edge to cloud applications bundle appliances and devices as horizontally scalable microservices that have to be geo-location aware and provide the data caching and processing close to the user. This calls for distributed flexible ad hoc up and down-scaling of compute resources and configuration. Such events may be triggered on demand or be scheduled.

The existing state-of-the-art cloud management frameworks use declarative definitions of the runtime environments and networks. Declarative means that the desired system state is declared in configuration files. The management system understands the status and applies measures to achieve the desired state.

In this context, the primary purpose of this focus area is to highlight the importance of considering common best practices for right-sizing and data centre infrastructure management, tackling design, simulation and prediction capabilities, as well as security and accessibility.

## 6.1. Technology Priority: Optimised Data Centre Design for Edge and Cloud

### Key drivers

Essentially, the basic building blocks for data centre infrastructure are available today but they lack standardisation and proper adaptation to the edge environment. This poses a management challenge to design, orchestrate, and scale distributed edge-cloud infrastructure.

One way of standardising infrastructure deployments is through sharing open reference implementations, also known as blueprints. There are many examples in the data centre industry, such as the OCP [79] which brings together data centre providers and infrastructure vendors to deliver data centre hardware solutions based on open blueprints. Another example is Anuket [97], which provides a common model and standardised reference infrastructure specifications for the telecommunications sector, including conformance and performance frameworks for virtualised and cloud-native network functions. More recently, SYLVA, another project at Linux Foundation, intends to deliver an open-source reference implementation of such cloud software infrastructure [94].

An important influence in the development of edge and cloud data centre blueprints should be regional conditions and requirements. In addition to obvious differences in climatic conditions in European countries, other possible local differences should also be included in the blueprints to be developed. These should consider several factors such as the current location (urban or rural environments), staff availability to operate data centres, power and network connectivity (especially with regard to possible expansion requirements), physical security requirements of the facility, proximity to manufacturing facilities (in particular if heavy work happens), or availability of industrial partners (e.g. waste heat consumers) in proximity to a data centre. These influential factors should lead to blueprints that can be flexibly adapted to regional climatic conditions, current environments and, if necessary, compliance requirements.

### Dependencies

Data centres and the physical networks are needed to operate services across the edge-to-cloud continuum. Therefore, they can be considered the backbone and neural system of these continua, which causes multiple dependencies. The most influential ones regarding data centre design and impact are:

*3.1. Technology Priority: Sustainability by* Design*:* The optimisation of data centre (designs) should include measures and amendments towards better repair / optimisation of components and IT equipment in order to extend lifetime of the components.

*3.3. Technology Priority: Code of Conduct for Energy* Efficiency*:* Using comprehensive and holistic metrics allows the evaluation, reporting, and optimisation of the overall sustainability and environmental impact of data centres.

### Relevant use cases / application domains

Given that a functional network of edge and cloud data centres is fundamental for an edge-to-cloud continuum in order to operate federated services, several use cases could benefit from the proposed recommendation. For example, in the *Public – Smart Cities* use case, the edge-cloud data centre may become a substantial integrated component in supporting sustainability goals, such as providing district heating. Furthermore, in the *Infrastructure – Edge-to-cloud Continuum* use cases, the data centre will provide the foundation for the infrastructure needed to run several applications and facilitate the requirements of data providers and users (e.g. in terms of data residency and data proximity).

### *Recommendations*

| | |
|---|---|
| *Short-term* | Continue supporting initiatives like the IPCEI-CIS [98] that are launching macro-projects to define reference implementations for the different layers in the edge-to-cloud continuum. More concretely, the ORECI macro-project will generate Open Reference Edge Cloud Infrastructure blueprints that will be key to building cloud and edge infrastructure and services that are open, distributed, sustainable, and highly scalable. |
| *Short/mid-term* | Promote the development and sharing of open reference implementations for different types of edge nodes. These types of developments and standards enable faster, more robust on-boarding into production, reduce costs, and accelerate digital transformation by facilitating the deployment of new edge data centre infrastructure with the right economy of scale to be competitive. European companies should collaborate in defining a set of open reference implementations that are fit for different types of edge data centre conditions: from urban to rural, near, far and on-premises edge, hot and cold geographies, supporting different types of processing (depending on the vertical demands in the area covered by the edge node), etc. This would contribute to achieving scale to compete with non-EU global players, facilitate interoperability and portability, as well as the development and deployment of infrastructure innovations coming from European providers. |

## 6.2. Technology Priority: Advanced Simulation and Prediction Capabilities for Operation

### Key drivers

It is important that organisations and edge data centre implementation projects address simulation and prediction capabilities to make them more effective and efficient in reducing their carbon footprints and to become more sustainable. By using simulation and prediction tools, organisations

can identify potential bottlenecks, predict future resource needs, and optimize the use of resources to reduce energy consumption and carbon emissions. Simulation and prediction tools can also support organisations to understand how their edge data centres are consuming energy, identify areas for improvement, and optimize their use of resources to reduce energy consumption and emissions. This requires the implementation of comprehensive and holistic metrics and the capability to predict future resource utilization to facilitate the planning and establishment of supply chains for anticipated demand to improve resiliency and implement a circular economy. This also allows organisations to evaluate their environmental impact, report on their progress towards sustainability which is demanded by legislation, customers and investors and continuously improve their operations.

Data centre infrastructure Management (DCIM) is the enabler to efficiently and proactively managing the capacity, consumption, and availability of all relevant data centre assets and components. It is also key to managing the growing number of data centre edge nodes, including servers, storage, networking, applications, power distribution units, heating and cooling equipment, security and building management systems. With the growing complexity AI capabilities will have to be integrated into DCIM to tackle the challenges in day-to-day operations of vastly distributed physical infrastructure, Digital twins and Building Information Modelling will also support the management and scaling of data centre infrastructure that consider certain local and sometimes adverse conditions.

Implementing advanced analytics to support innovative, real time DCIM for capacity planning, VM rightsizing, rightsizing the container environments, energy consumption monitoring, rack temperature data, etc. will help to reduce the human effort and improve security, accuracy, and efficiency of the environment. Machine Learning can also help detecting problems faster or even preventing them, reducing carbon emissions and resource consumption, maintaining the infrastructure proactively and improving return of data centre investment.

On the other hand, data centres need huge investments in capital expenditure expenses and OPEX. Data centre design effectiveness is becoming more critical; therefore, many organizations seek to cut back, with the goal of reaching net-zero carbon emissions and a good return of data centre investments. Additional innovative solutions and commercial solutions can be a key differentiator in the data centre infrastructure. Research firm Gartner predicts that half of cloud data centres will be leveraging advanced robots with AI/ML capabilities by 2025, and AI-centred deployments will ramp up the operating efficiency of data centres [88]. Analytics and AI/ML for infrastructure management can help to manage data centre IT processes in an enhanced way. To this end, it is necessary to capture and analyse in real time data from data centre processes and device information through software and hardware infrastructure sensors, which will then be used by AI/ML models. These sensors provide data regarding temperature, thermal maps, heating, humidity, airflow sensors, water temperature, smoke, electricity, power, room entry, environmental footprint, rack provisioning, server health management, and they are located along all the premises, infrastructure, and at the servers.

With all the relevant data gathered and analysed this enables several approaches providing simulation capabilities. Thus, this knowledge and best practice can be utilized in Digital twins and augmented reality for simulation, reducing the operational risk and analysing "what-if" scenarios, with the aim of modelling and optimizing layouts before investments being made and they materialize in the data halls. Energy modelling tools and building performance simulation (BPS), which allow engineers to understand the behaviour of airflow and heat transfer within data centres spaces, allow the prediction of energy consumption and can evaluate the effects of the inclusion of renewable energy options (e.g. solar panels) and the selection of sustainable materials. DCIM Tools and platforms for monitoring and operation which allow the configuration of dashboards to display the data and KPIs needed for planning and decision-making including drill-down mapping that evolves from a data centre-wide to a cabinet-level view, providing a detailed mapping that shows smart rack sensors such as thermal maps. There are quite a number of key drivers in both simulation and prediction capabilities, and there are several tools and techniques to achieve these ends, such as digital twins, augmented reality, simulation software, building orientation, energy modelling with a building performance simulation (BPS), Building Information Modelling (BIM) system, and DCIM and computational fluid dynamics (CFD) tools.

### Dependencies

Data centres and the physical network can be considered the skeleton and nerves of the edge and the edge-to-cloud continuum. Both are needed to operate services across these continua. This creates multiple dependencies. Given the topic of this subsection, we would like to highlight the most influential ones regarding data centre design and impact:

*3.3. Technology Priority: Code of Conduct for Energy* Efficiency*:* Utilising comprehensive and holistic metrics in data centres DCIM and digital twins enables evaluation, reporting, and optimization of the overall sustainability and environmental impact of data centres.

*3.4. Technology Priority: Use of Digital Technology* as AI/ML*:* Supports the optimisation of data centre operation, reduces costs and the environmental impact, and increases resilience.

### Relevant use cases / application domains

Given that a functional network of edge and cloud data centres is fundamental for an edge-to-cloud continuum in order to operate federated services, several use cases could benefit from the proposed recommendation. For example, in the *smart cities* use case the edge-cloud data centre may become a substantial integrated component as it would support sustainability goals by providing heat for district heating. Furthermore, in *infrastructure-related* use cases, the data centre will provide the foundation for the infrastructure need to run several applications and facilitate the requirements of data providers and users (e.g. in terms of data residency and data proximity).

Moreover, utilising the concepts and ideas of the *AI federated machine learning* use case supports utilisation of the collected data and, consequently, the development of AI-powered data centre operation and orchestration applications.

***Recommendations***

| | |
|---|---|
| *Short-term* | Implement real-time monitoring and reporting of energy consumption on every level of the data centre operation. One of the key drivers for implementing advanced simulation and prediction capabilities is the need to understand and optimise the energy consumption of edge data centres. |
| *Mid-term* | Develop comprehensive simulation models such as digital twins, augmented reality, simulation software, building orientation, energy modelling, and AI/ML platforms for data centre infrastructure, to manage data centre IT processes in a more proactive and predictive way. This will improve data centre efficiency, manage SLAs efficiently, detect problems faster, reduce carbon emissions and footprints, propose proactive maintenance tasks and generally reduce resource consumption and improve return of data centre investments. |

## 6.3. Deployment Priority: Edge Data Centre Security and Accessibility

### Key drivers

Due to the distributed nature, smaller size, and remote location of edge data centres, the aspects of security and accessibility become a challenge. To solve these challenges is particularly important when edge data centres become critical infrastructures for applications such as in energy supply, human-machine interaction or mission-critical business processes, etc.

Not all proven security management methods of large-scale data centres can be down-scaled easily to fit into edge environments and so the data centre industry has to consider new security approaches in order to maintain physical and access security, facility security, and cybersecurity.

In order to run edge data centres remotely, the following measures should be enforced, especially when remote locations are not permanently staffed with on-site engineers: (i) management and best practices of physical security, through best security standards and practices that must be followed in order to design and execute a secure data centre, (ii) protection and monitoring of facility security, by establishing the mechanism to monitor those related to design standards, security, redundancy and other data centre building constructions aspects, and (iii) proactive cybersecurity prevention and detection, by focusing on controlling access to enterprise data and applications hosted within the data centre's IT infrastructure, ensuring that only properly authenticated users can access data or use applications, and that any breaches are reported and addressed immediately and using proactive detection systems (anti malware, configuration management, intrusion detection, activity logging and other tools) to oversee network activity and identify potential threats.

In the context of data centre infrastructure, the supply chain aspect should be noted. It is required to validate the authenticity of newly introduced software, software updates and devices including

their firmware and updates from central nodes. For instance, if the swapping of hardware on remote sites is done by contractors, the central validation of authenticity of them must be possible. In addition to software and logic security risk (cybersecurity, hacking, antivirus, firewall, software update, communications, etc.), there are also other important area to focus on like the data centre and Edge Physical security to minimise vulnerabilities and business disruptions.

Regardless of the size, an organisation´s data centre, is always at risk of being vulnerable, either intentionally or accidentally. Therefore, as many security measures as possible must be taken to allow the organisation to create a robust digital infrastructure and diagnostic security plan that enables a resilient business continuity management that will address physical risks such as: voltage rises or drops, incorrect temperatures due to failure of air conditioning equipment or poor design, fire, floods and humidity, air quality, access by unauthorized personnel, improper handling of equipment, vandalism, theft, seismic movements, etc.

There is a requirement both for standards regarding the elimination of key security vulnerabilities and for approaches related to verification and validation given that trust chains that can be scaled in the cloud-edge continuum need to be established as well as standardized QA processes and roll-back capabilities for updates and upgrades. Moreover, automated and continuous penetration testing and regression testing on publicly known vulnerabilities is required to increase the corresponding security levels, complemented with best practices for integrity, reliability, and security for each abstraction layer. Implementing these measures will foster a state of the art zero trust architecture.

### Dependencies

As edge data centres become critical infrastructure, customers and users become more sensitive to data security and legislators are increasing the requirements and penalties for ensuring data security by organisations, having appropriate security measures in place is critical. Since the edge data centre is only one link in the security chain, the most important dependencies for enabling end-to-end edge data centre security are listed below:

*2.7. Technology Priority: Promote & Implement Local* Processing of Data*:* Independent and local processing of date requires a secure data centre, both regarding the unauthorised access to a remote site and the logical access to the applications by bypassing network access.

3.4. Technology Priority: Use of Digital Technology as AI/ML*:* This may also be used for threat detection in the case of suspicious or unusual data traffic, power consumption or climate control.

*4.4. Deployment Priority: EU automated Security Operation Centres (SOC) for Faster Detection & Response to Cyber-attacks from Cloud to* Edge*:* EU automated Security Operation Centres (SOC). This is quite relevant since it would enable faster detection and response to cyberattacks from cloud-to-edge.

### Relevant use cases / application domains

Given that a secure network of edge and cloud data centres is fundamental for an edge-cloud continuum in order to operate and maintain critical federated services, several use cases will benefit from the proposed recommendation. For example, in the smart cities the edge data centre will enable real-time data processing needed for smart grids and mobility use cases which supports local and regional sustainability goals. Furthermore, in infrastructure-related use cases, the data centre will provide the foundation for the infrastructure needed to run multiple secure applications and facilitate the requirements of data providers and users (e.g. in terms of data residency and data proximity).

The importance and the need for a trustworthy supply chains for components and IT equipment is reflected in the digital supply chain use case, since the data centre operator should be able to check the authenticity of components, IT equipment, and related software artefacts in real time.

### *Recommendations*

| | |
|---|---|
| *Short/mid-term* | Leverage cross-site mirroring of software updates and roll-back capabilities. Following the paradigm of having the same configurations across all edge sites makes it less likely that a single site will be compromised undetected. Stringent enforcement of fine-grained security policies including cascading down across abstraction layers and Role-Based Access Controls (RBAC), will ensure that different principals have different visibility and control over the underlying abstract objects. |
| *Mid-term* | Introduce standards for the enforcement of key elements, addressing the key security vulnerabilities that can be caused due to the limitations of distributed and remote sites. This will allow operators to certify their contractors and hardware suppliers, and to introduce processes for auditing and compliance. |
| *Mid-term* | Oblige integrators in the context of European OCP projects to adopt the certification standards and ensure that the authenticity of every downloaded component can be certified. Introduce quality and security validation processes and principles to prevent the introduction of malicious code via open source projects. For example, a PaaS provider should not have to check if the underlying infrastructure is not corrupted, nor should the provider need to know about the origin of the underlying hardware. |

# Focus area: Reducing the Environmental Footprint

It is important that organisations and data centres address sustainability and reduce their environmental footprints. Data centres, in particular the hosted IT platforms, consume a great amount of energy and resources and they are one place where many organisations seek to cut back with the goal of reaching net-zero carbon emissions. Energy consumption and overall environmental sustainability have come into focus and data centre operators are making commitments on sustainability as part of their Environmental, Social, and Governance (ESG) programmes.

## 6.4. Technology Priority: Energy Optimisation and Resource Conservation

### Key drivers

The rising costs and demand for energy supply and rare resources put economic and ecological pressure on the edge-to-cloud data centre landscape to optimise its energy efficiency in the following areas: energy, cooling and heat usage, renewable energies such as solar and wind, energy storage like green hydrogen, and new types of batteries to be integrated into edge cloud deployments. Waste heat on the other hand can be integrated into local and district heating, industrial applications, or biogas plants.

To enable and support these new approaches, actors from all relevant sectors (e.g. municipalities, utilities, data centre industry) have to collaborate in inclusive project approaches that prioritise integration and synergies to generate added value. While data centre operators need to overcome some significant challenges that they cannot solve individually, the availability of edge data centres can greatly support the provision of Smart Grids and IoT to foster the integration of (renewable) energy supply, optimise resource life cycles, and support efficiency in other sectors as well. Edge data centres also reduce the energy needed for data transfer while being closer to the data producer and consumer.

For example, a segmented approach in IT Operation can deliver the ability to put unused elements into deep sleep and therefore avoid “idle” power waste. Modularization and componentization also enable continuous upgrade activities based on technology advances and matching customer demands.  Another area of potential efficiency gain is the extension of the Battery Backup (UPS) so they can be used as integral component of Community Batteries or electrical Charging Stations.

Additionally, the utilisation of advanced technologies, such as neuromorphic computing, in hardware design has the potential to enhance the sustainability of computational systems. This is achieved by enabling more energy-efficient computation for specific workloads, thereby reducing the carbon footprint and promoting sustainability in the long run [100].

The data centre industry is already implementing several initiatives such as high energy intensity, rapid growth, large power consumption, cooling, and water usage. But these are mainly concerned with managing the actual hardware infrastructure of data centres. The areas that must be addressed, however, are the facility to host the data centre, IT to run the operation, and the cloud hardware itself (compute, storage, and network) in an integrated, cross-sector approach. To tackle the growing demand for rare resources needed in the data centre infrastructure and IT, asset life cycles can be prolonged; they can be repaired or refurbished to be used again before finally being recycled.

### Dependencies

*3.1. Technology Priority: Sustainability by* Design*:* Integrating circular economy methods into data centre infrastructure will enable significant efficiency gains in energy and resource consumption.3.4. Technology Priority: Use of Digital Technology as AI/ML*:* While data centres have helped to make AI accessible to organisations, data centre operators need to implement AI to optimise their infrastructures and services efficiency.

*3.5. Deployment Priority: Data Centre* Metrics*:* easily applicable and understandable *Data centre metrics* are needed to establish KPIs that can be monitored and managed through advanced analytics to improve and report operation and efficiency gains.

### Relevant use cases / application domains

Edge data centres are a key building block for *Public – Smart Cities* digital infrastructure. They enable smart grids for renewable energy implementation and distribution. Integrating data centre´s waste heat into local and district heating, or making it available for agricultural and industrial applications, supports reducing the environmental footprint in other sectors as well. Manufacturing and production industries foster the implementation of data centre grids in their infrastructures by activities like the Open Direct Current Alliance (ODCA).

## *Recommendations*

| | |
|---|---|
| *Short-term* | Establish sustainability plans for data centre operators based on standardised and specialised metrics that will foster adoption, improve benchmarking, and progress sustainability within this industry. Utilise holistic sustainability key metrics for data centre infrastructure and IT, and also consider the whole life cycle including rare resources to identify and realise optimisation potentials. Implement data centre sustainability plans to comply to local, national, and EU-wide sustainability plans so as not to jeopardise the overall efforts and goals. |
| *Mid-term* | Optimise energy and resource consumption by implementing Circular Economy methods and increase facilities' efficiency by implementing AI in data centre operation. Emphasize and incentivise innovative, sector-overarching approaches by fitting and making use of local regulations, requirements, and opportunities |

| | |
|---|---|
| | that foster operational efficiency. Optimise the use of renewable energy and resources, and find customers for waste heat to provide further environmental benefits. |
| *Long-term* | Many optimisation opportunities depend on the collaboration of infrastructure providers and the availability of the required infrastructure, e.g. local and district heating or smart grids. The challenges to be solved will be how to connect data centre to the necessary infrastructure while available space in cities is scarce and infrastructure projects are expensive. At the same time, moving data centre out of the cities will require even bigger investments in infrastructure and might circumvent some optimisation opportunities. A good example to demonstrate the issue is the implementation of green hydrogen for (data centre) energy supply, which is more feasible in Greenfield edge data centre deployments, rather than Brownfield data centre in city centres. |

## 6.5. Technology Priority: Rethinking and innovating Design for Sustainability

### Key drivers

To achieve a higher sustainability for existing data centres, architectural changes have to be applied to decrease the power consumption and the environmental impact of data centre operation. For new data centres integrated designs need to be implemented to foster strong sustainability and allow circular economy. These new designs and approaches also enable new business models that benefit DC operators and customers. Integrating alternative, at best renewable resources to build the data centres infrastructure makes data centre deployments more resilient to and independent from supply chains and helps to acknowledge local requirements and opportunities. For example, the data centre´s energy backup systems can be integrated to stabilize smart grids and vice versa.

Today, considerable effort is already undertaken to make use of waste heat for local and district heating, agricultural or industrial applications. This seems obvious since 60-70% of the data centres´ energy demand will be transformed into waste heat. To maximise added value here, data centre operators need to partner with cities and look for customers with a constant demand for heat which fits the data centre´s output (public swimming pools, drying bio mass, growing algae, asparagus, fish or maggot farms for food production). New data centre designs will also have to consider different ways of cooling (air or liquid), heating (floor) and lighting (on demand or none at all). This can have an impact on the waste heat output temperature and helps fit local and customer requirements and mitigate demand for heat pumps.

New demand for edge and real-time applications affects and challenges the ability of (edge) data centres to enable these applications (e.g. human-machine interaction, autonomous cars or drones, real-time decision making in production and infrastructure maintenance). Therefore, new methods and AI capabilities have to be implemented in the real-time orchestration and operation of

demand-based workload management of each edge node, as well as the distribution/transfer and storage of the relevant data across multiple sites.

### Dependencies

*3.3. Technology Priority: Code of Conduct for Energy* Efficiency *in Data Centres:* This is necessary to raise awareness of the many options that exist to improve not only energy efficiency, but also strong sustainability in order to attract attention by all relevant actors and to realise holistic and feasible design approaches.

*3.4. Technology Priority: Use of Digital Technology* as AI/ML*:* The implementation of AI technologies for data centre operations is needed to support sustainable and innovative data centre designs.

*3.5. Deployment Priority: Data Centre* Metrics*:* to verify and report design improvements, holistic *Data centre metrics* and comprehensive KPIs that can easily be monitored, managed and reported are needed.

### Relevant use cases / application domains

Sustainable designs support the decentralised deployment of edge data centres as described in the *technology use cases,* in particular infrastructure and telecommunication. These designs will enable competitive disadvantages for edge data centre providers to be avoided, mitigating resistance in the public domain (for instance municipalities) to provide the necessary space and support to integrate edge data centre in the local infrastructure and for the acceptance of this by citizens.

### *Recommendations*

| | |
|---|---|
| *Short-term* | Raise awareness of successful, sustainable designs and foster collaboration among all relevant actors. Support research and implementation of innovative data centre designs and increase use of building performance simulation (BPS), Building Information Modelling (BIM) systems, Data Centre Infrastructure Management (DCIM) and Computational Fluid Dynamics (CFD) tools. |
| *Mid-term* | Update regulations and requirements for data centre operations to meet EU-wide and national sustainability goals in order both to avoid competitive disadvantages for data centre operators and to foster the deployment of sustainable data centres. Therefore, data centre metrics have to be extended and standardised. Fit reuse of waste heat through desirable output temperatures via air or water cooling to match local heat demands and applications. |
| *Long-term* | Support use of waste heat in local and district heating through a collaborative and integrative implementation of an infrastructure by all relevant actors. Integrate the use of green hydrogen to compensate for fossil fuels for data centre energy |

supply and backup-energy, therefore new external infrastructure for the use / transport of hydrogen has to be implemented as well through collaboration of municipalities, utilities, and data centre operators. This also requires research in the area of efficient green hydrogen production and provision to be feasible and cost efficient.

## 6.6. Deployment Priority: Delivering Sustainable data centre Blueprints

### Key drivers

In 2022 a survey conducted by IDC found that European organisations strongly favour a private IT infrastructure with just 2% of the organisations using only the public cloud and 10% preferring the public cloud over a private IT infrastructure or a mix of both worlds. This is a huge opportunity for the European cloud industry to meet this demand with sustainable, trusted and resilient edge and cloud infrastructure. To realise this huge opportunity, all relevant actors from research to industry will have to collaborate with municipalities, utilities, public authorities and customers in an ecosystem that benefits all parties. Future decentralised, diverse edge data centre designs, not to mention the projected number of facilities and their integration into the computing continuum, will introduce many new requirements that need to be addressed. In order to meet these requirements and achieve the European goals for sustainability, data sovereignty and cloud infrastructure, a large number of different data centre blueprints must be created and tested in practice in order to meet the demand for IT infrastructure in the respective Member States.

In order to be able to serve the increasing demand for (local) data centres and to achieve the sustainability goals with competitive solutions that take local requirements and regulations into account, innovative data centre designs must be implemented and tested in practice. These designs should serve as blueprints that draw attention to more sustainable solutions and disseminate the knowledge, serving also as examples and best practices outside the EU. Unfortunately, there will be no one-size-fits-all blueprint. While it is already challenging to implement new designs in greenfield projects, it becomes even more challenging to adopt these in established data centres, especially when they reside in dense urban areas. The ultimate goal is to find solutions that can be implemented into stock data centres, while having to make only minor changes to the existing designs and architecture.

The major challenges are in the use of renewable energies and materials, the use of waste heat and implementing a circular economy, realising efficiency gains, introducing modular and scalable designs while ultimately maintaining competitiveness or even having an edge over competitors.

### Dependencies

*6.5. Technology Priority: Rethinking and* innovating Design for Sustainability*:* Applied research has to be conducted in new and existing data centres to foster the deployment of sustainable and innovative data centre designs.

### Relevant use cases / application domains

All *technology use cases* have to be integrated and applied to achieve the desired sustainability goals. Thus, new data centre design blueprints will be impacted by the development in these domains and vice versa given the complete data processing lifecycle (and the respective actors).

## *Recommendations*

| | |
|---|---|
| *Short-term* | Apply holistic metrics and test new design approaches in edge data centres where the investment is comparably low. Collect over the whole life cycle all the relevant data from the facility, the IT assets and operation. Examine the results for improvement, feasibility and applicability for stock data centre. |
| *Mid-term* | Apply successfully tested concepts to stock data centre – one at a time for comparability – and measure efficiency gains and success there. Disseminate results and identify already successful designs. Keep improving designs. |
| *Long-term* | Foster integration of successful designs in stock data centre through dissemination, regulation and incentives. |

# SECTION 7: A NEW CONNECTIVITY FOR THE EDGE AND CLOUD

As forecasted by the European Data Strategy, the global data volume will increase from 33 zettabytes in 2018 [101] to 180 in 2025 [102]. Efficient and performant interconnectivity will play a key role in providing a well-established networking infrastructure that meets the requirements of a digitalised and data-driven society and that supports the associated traffic capacity demand - expected to scale up to the zettabyte order of magnitude.

Furthermore, mobile devices will be the predominant means of accessing applications across the edge-to-cloud continuum. The number of these devices and the corresponding connections grows constantly: 25 billion Internet of Things (IoT) devices, 2 billion 5G connections, 70% mobile coverage worldwide, and mobile broadband adoption of 95% are expected by 2025 [103]. A good part of the connections will come from IoT, not just from humans, and both will require an optimal path from the device to the edge computing resources for some of the device applications to perform.

Thus, fixed and mobile access, core and transport networks will have to evolve to connect the new computing nodes with the characteristics demanded by many edge applications: (i) *high reliability and uptime* through a resilient connectivity infrastructure [104], (ii) *secure* and *well-performing* services through the configuration and assurance mechanisms of the mobile network, (iii) *close-loop* and *automation* features through mechanisms like network slicing and orchestration among all platforms at scale [105], (iv) *interoperability* and *portability* of the connectivity solutions through a standard Software-defined access, via Network-as-a-Service APIs [106],[107] that also enables enhanced business outcomes (develop once, deploy everywhere), and (v) *trust* and *security* through mechanisms for control and isolation of data and traffic, that facilitate data protection and sovereignty requirements and ensure data locality (e.g. data stored in Europe) and traffic locality (i.e. traffic to/from the edge node stays in Europe and is isolated at network level) [108].

The aforementioned evolution addresses the network architecture and technology (5G user plane, virtualised RAN, software-defined transport network, time-sensitive networking, etc.) and aims at covering not just the device connectivity but also the connectivity among the nodes in the edge-to-cloud continuum, and between different providers to enable service federation. These core priorities are depicted in Figure 16 below.

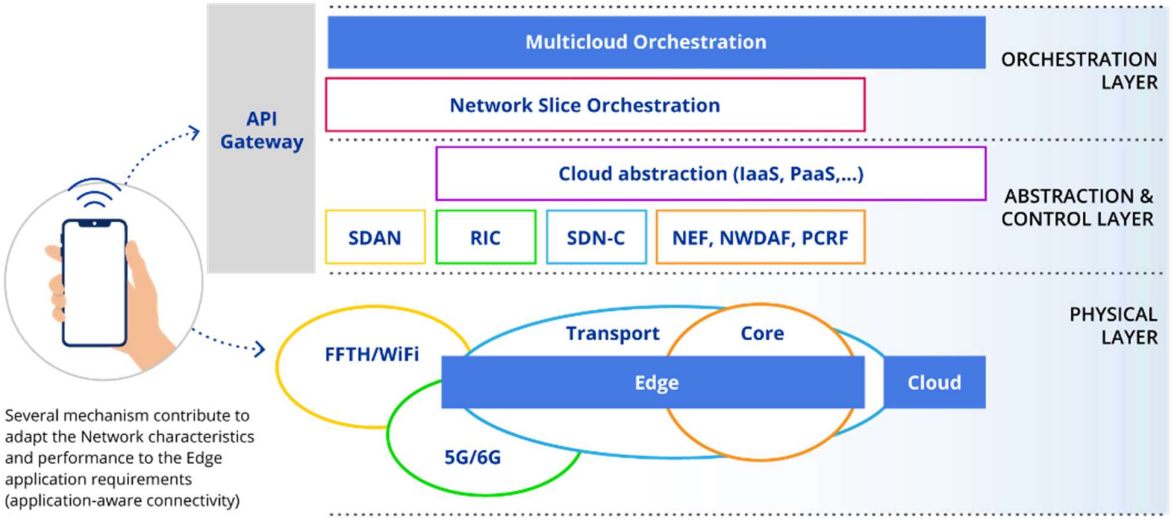



*Figure 16: Priorities for a new connectivity for the edge and cloud continuum*

Overall, Europe's edge and cloud facilities will require advanced *network management and orchestration* technologies, exposure of network capabilities as well as *interconnection services* to guarantee efficient infrastructure utilisation and enable innovative edge use cases at scale. The European market must also adopt cloud native technology in both its fixed and mobile networks (such as FTTH/Wi-Fi and 5G), leveraging the global competitiveness of its network equipment providers and the global footprint of its telecommunication operators to transform the mobile network into a backbone for a network of widely distributed edge nodes.

# Focus area: Optimal device connectivity to the edge

## 7.1. Technology Priority: Device Connectivity for a True Edge Experience

### Key drivers

To deliver the right performance and requirements, the edge infrastructure needs to be properly and safely connected to the cloud and to the customer. Optimal connectivity is important to deliver a competitive edge cloud service for most of the edge applications (e.g. those having strong latency, jitter, throughput, or security requirements). For such applications, the users' experience depends on the respective computing quality and performance but also on a stable and quality edge connectivity, as many of their requirements rely on it.

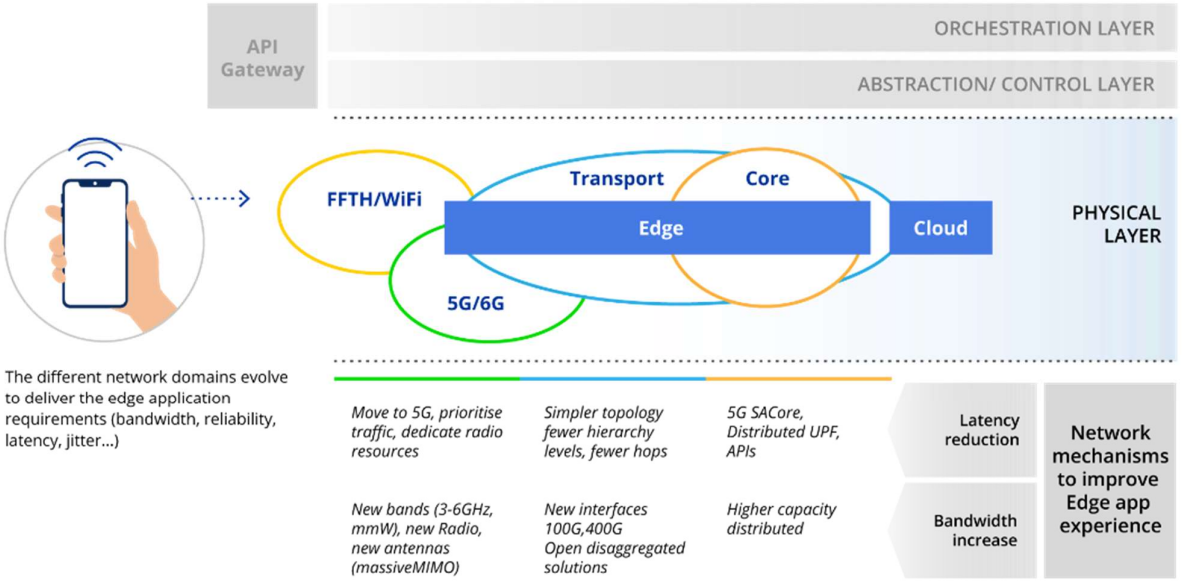
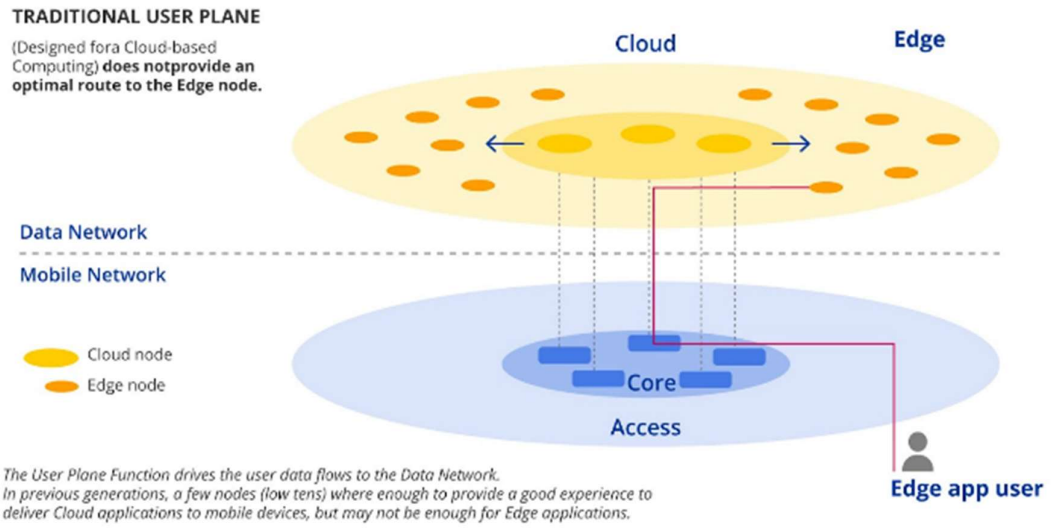



*Figure 17: Measures at network level to improve edge application experience*

Even though every new mobile generation has brought latency improvements on the radio interface [109], the rest of the radio network has been designed to optimise the use and performance of the installed radio capacity (load balancing, congestion avoidance, etc.), without taking into consideration parameters like *latency* or *jitter* [110].

Additionally, previous generations of radio network technology provided generic functionalities for all services, designed to provide all concurrent users with equal access to all the installed capacity. 5G technology allows the provision of a customised network experience with programmable Quality of Service that allows the user to change it on demand, using capabilities like *Network Exposure Function* [111] or *Network Slicing* [112].



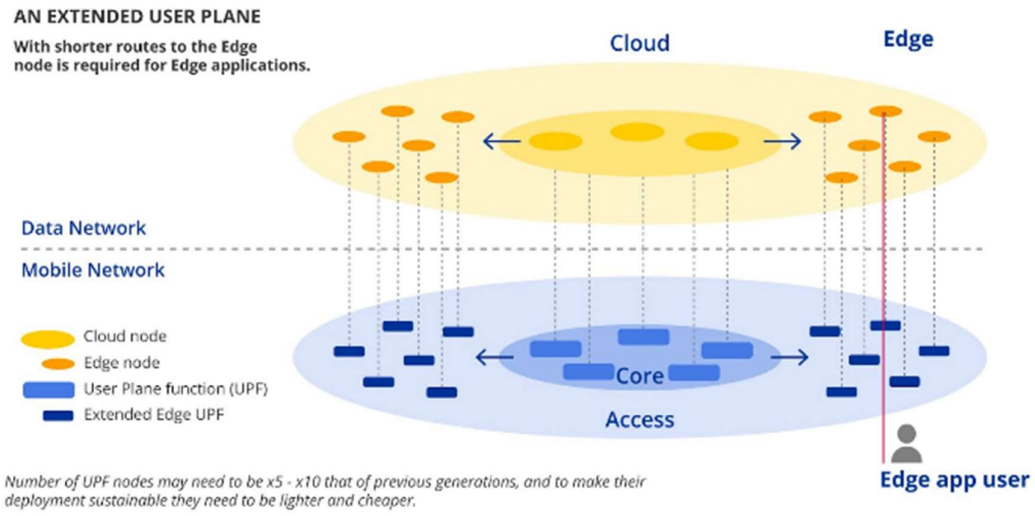



*Figure 18: From traditional to extended User Plane function*

### Dependencies

This focus area does not present relevant dependencies with other priorities in this roadmap, beyond the need to fulfil the requirements of the different edge applications.

### Relevant use cases / application domains

*Remote AR-based professional support* will require certain upstream bandwidth to deliver the live video stream to the remote specialist and very low latency to be able to render and stream the AR image back on the glasses of the field technician to assist him or her in real-time.

*Immersive video experience* and *Virtual Reality entertainment* will require high downstream bitrates and low latency to provide a good experience and avoid motion sickness.

## *Recommendations*

| | |
|---|---|
| *Short-term* | *User plane functions* (UPF) provide access to the data network, i.e. the computing nodes, and are currently fit for cloud applications (deployed only in a few locations) but not for low-latency edge ones. They will have to be more *distributed* (i.e. one UPF element for each edge node), to be closer to the edge application to deliver latency and efficiency to edge applications, and will have to be simplified, as 5-10x more elements are expected. The *cloudification* of the user plane function (UPF as cloud-native function, CNF) will facilitate this distribution process, allowing it to be more dynamic and on-demand. |
| *Mid-term* | The *cloud-native* evolution of the access (fixed and radio access networks virtualisation and emergence of the RAN Intelligent Controllers) and transport (consolidation of the software-defined network controllers) domains will facilitate |

| | |
|---|---|
| | the end-to-end control of the user connectivity by enabling the creation of specific dynamic network slices. |
| *Mid-term* | The complexity of managing a more distributed user plane is higher and requires more interactions at the control plane, an overhead that may have an impact in terms of congestion and latency. *Automation* will be essential to deliver the user plane function efficiently and keep it under control, avoiding issues like reconfiguration overhead that may affect the Core Network by using mechanisms like Dynamic Placement and Chaining Reconfiguration [113]. |
| *Mid-term* | To move towards allowing customers to benefit from a dedicated service and fulfilling their requirements, *network capabilities* like Quality on Demand or Network Slicing should be *exposed* to the edge customer in a simple fashion through APIs allowing a straightforward integration between network capabilities and cloud services. These APIs enable E2E services that encompass both the telecommunication services and the cloud ones, i.e. 5G Edge Cloud services. |

## 7.2. Technology Priority: Control & Orchestration for Edge Connectivity at Scale

### Key drivers

The delivery of latency, bandwidth, privacy, and security requirements of certain edge applications will require in many cases the allocation or prioritisation of certain network resources for certain customers, some of them scarce like the radio resources. This cannot be addressed without the necessary adaptation of the telecommunication networks. Offering that *at scale* to customers will require *automatic*, *on-demand*, and *as-a-service* mechanisms to monitor and control the network performance while optimising network resource consumption and investment, in such a way that resources are allocated only when and where they are needed and only for the customers and applications that require them.

Standard mechanisms to enable a *dynamic connectivity control*, like traffic management, bandwidth allocation across the edge-to-cloud continuum or simple access to network and device status information, are missing.

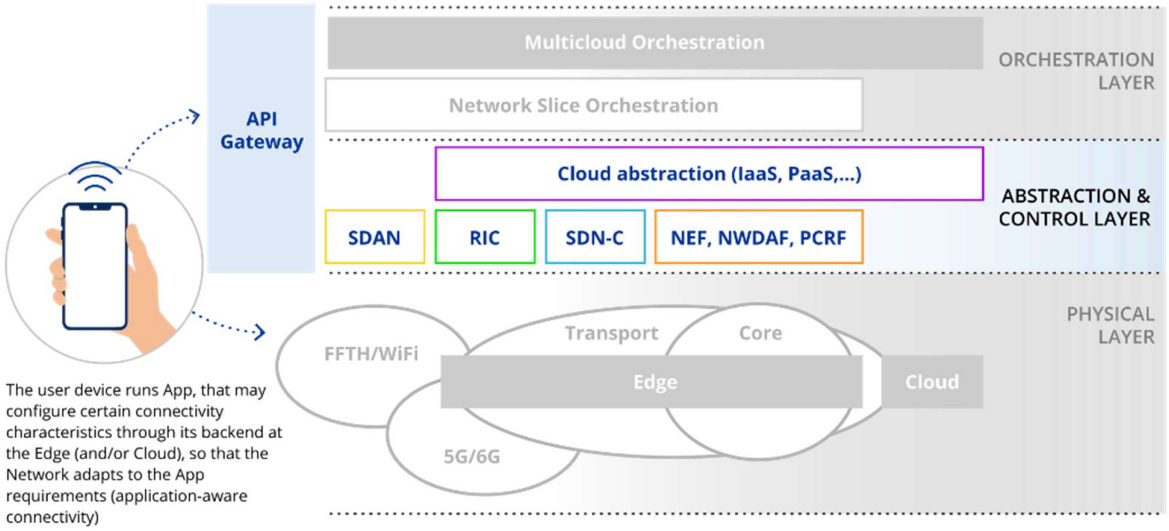



*Figure 19: Network capabilities abstraction and exposure via an API Gateway*

New software components need also to be developed and standardised. These components will deliver to application developers and business customers features in a cloud-like, easy-to-consume way, i.e. through Network-as-a-Service, NaaS APIs. Such features include traffic management, network orchestration, monitoring and quality of service assurance. For example, CAMARA, an open-source project launched at Linux Foundation in collaboration with GSMA [93], plays a key role in this standardisation process, which communication service providers will have to contribute to.

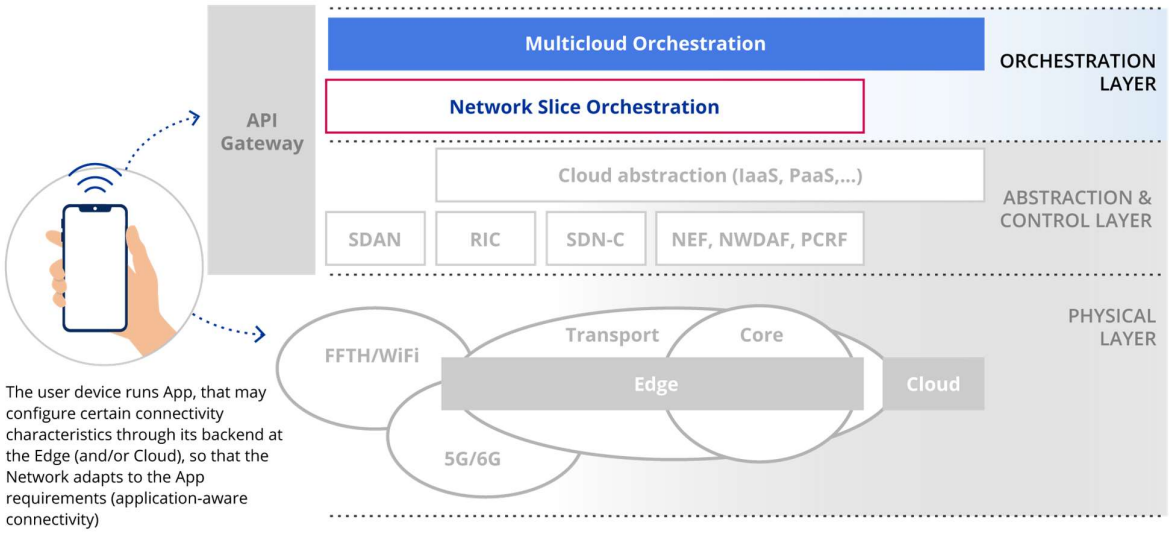



*Figure 20: Network orchestration for dynamic necessary edge and cloud connectivity*

Furthermore, the current lack of *multi-cloud/multi-network cross-border orchestration* (as also addressed in Section 5), leads to a market fragmentation that benefits global cloud service

providers and limits the opportunities for smaller service providers. *Open orchestration and assurance* solutions are not available. Solutions nowadays are proprietary and closed. There is an option and, indeed, a need to tackle the latter, contributing to Europe's vision on data and digital sovereignty.

### Dependencies

*7.1. Technology Priority: Device Connectivity for a True Edge* Experience*:* The API capability exposure will be fundamental for an automated orchestration of network services, and the evolution of the network, as it becomes software-based and cloud-native, will facilitate it, as cloud automation tools and techniques can be applied.

*Focus area: Orchestration and Federation of Distributed Edge Cloud:* The network deployment and operation will benefit from the availability of means to orchestrate and federate hybrid multi-cloud environments.

### Relevant use cases / application domains

The possibility to apply certain traffic prioritisation can be of high value for *public safety services* that require high levels of availability and specific network capabilities in certain critical situations.

*Enterprise communications* experience could be enhanced if the quality of service can be guaranteed along a group videoconferencing session.

### *Recommendations*

| | |
|---|---|
| *Short-term* | *NaaS platforms* to allow the network capabilities to be opened to edge customers and applications on-line, on demand, through open and standard APIs, in a controlled and safe way. This enhanced control will be facilitated by the cloudification of the network and technologies like Software Defined Networking (SDN), that abstracts the control layer from the network elements. Communication service providers should design, develop, and implement these NaaS platforms as *API gateways* [114], abstracting and exposing the network capabilities to the customers. |
| *Short/mid-term* | Develop *NaaS APIs*, supported by new cloud-native, software-based technologies like the 5G Stand-Alone Core [115], to provide the means to implement the access to specific network capabilities for edge and cloud application developers more efficiently. As they demand a high consumption of resources, Application Services will have to request them on demand, only where and when needed. The standardisation of NaaS APIs, in bodies like GSMA, Linux Foundation or TM Forum, is key to achieving *interoperability*, enabling *multi-vendor solutions*, wide availability (implementation by communication service providers) and *adoption* (usage by customers such as edge application developers). |

| | |
|---|---|
| *Long-term* | Establish *mechanisms* and *interfaces* to secure performance across network-cloud deployments when providing cross-regional services, and be agnostic to the underlying edge, cloud, and network infrastructure. To deliver the E2E network orchestration, *network-centric AI models* and their corresponding life-cycle management will have to be developed. The softwarisation and cloudification of network functions and resources is enabling a more dynamic and flexible management of network services. This *network management and orchestration* will have to be tightly coupled (i.e., coordinated and integrated) with the edge and cloud orchestration to provide a proper connectivity service across the edge-to-cloud continuum (see Sections 5 and 9). This coordination needs to be addressed and automated in an end-to-end way across different layers: service, resource, and infrastructure. |

## 7.3. Deployment Priority: Deliver a Performing Device Connectivity to the Edge

### Key drivers

The mechanisms to couple the edge nodes and platform with the Mobile Network are being tested and standardised in bodies like GSMA [116], ETSI [117], MEF [118], or 3GPP [119]. This standardisation process is expected to be completed by 2022-23 and its deployment will represent a significant adaptation effort for the Mobile Networks. As depicted in the figure below, the user plane function *needs to be implemented in each edge node to fulfil latency, jitter, and security requirements*. This may represent a significant operational and economic effort (the number of user plane nodes could be increased by 5 or 10 times), having to adapt many network nodes in terms of topology, technology, capacity, and infrastructure to deliver a sustainable solution.

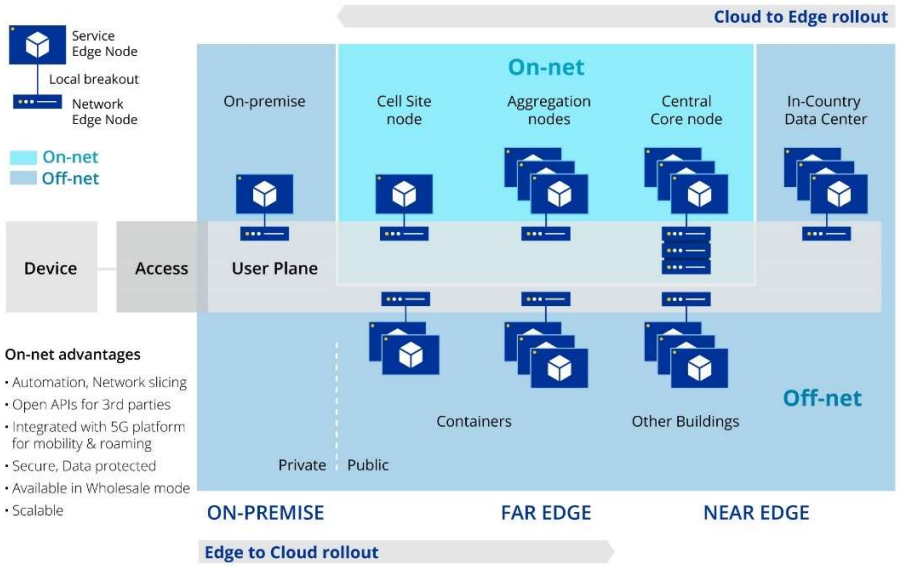



*Figure 21: User plane function provides a fast local breakout to the edge node at every location*

Furthermore, the user plane function connects the user, attached to the mobile network, to the data network, where edge and cloud nodes are hosted. For customers connected through a fixed access network, the challenge is relatively simpler. These customers are statically assigned a Far or Near Edge node for running their edge applications depending on their requirements (latency, residency, etc.). Nevertheless, the deployment of connectivity for fixed access customers will also be costly as connections to the cloud, now made at the highest levels of the transport network (interconnection level), will have to be complemented by connections to edge nodes at other levels of the transport network hierarchy (transit, service, or aggregation, depending on latency requirements) and this means additional hardware in these lower levels.

### Dependencies

*7.1. Technology Priority: Device Connectivity for a True Edge* Experience*:* It will deliver the solution to transform the network in a way that delivers the required efficiency and performance for the edge applications.

*7.2. Technology Priority: Control & Orchestration for Edge Connectivity at* Scale*:* This will facilitate the provision of the required connectivity on demand and "as a service" in a sustainable and scalable way, as required for a massive edge deployment.

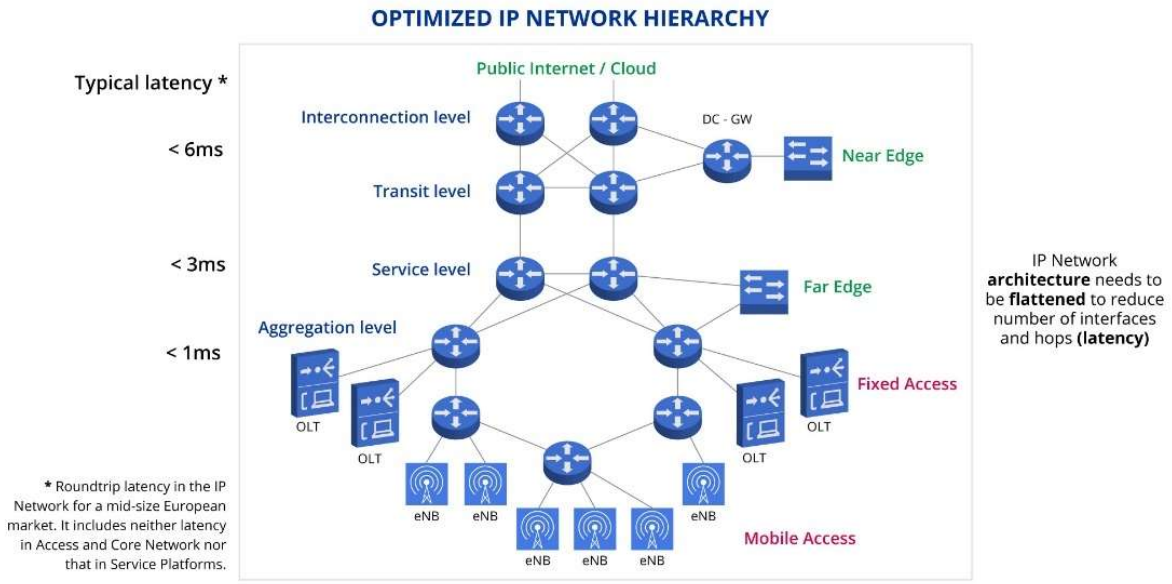



*Figure 22: Edge connectivity to fixed and mobile access networks*

### Relevant use cases / application domains

*High-Definition* (8K) and *Immersive* (360º) *video streaming* require the transmission of high volumes of data, incurring high transport costs. It will be highly benefited by moving the streaming servers closer to the edge over an optimised transport network.

An even more demanding case is that of *cloud XR game streaming*. This also demands an ultra-low latency to transmit in real-time the change in the position and direction of sight of the user (6 degrees of freedom) to render and stream the adequate image.

### *Recommendations*

| | |
|---|---|
| *Short-term* | The *user plane* will have to be *extended to the near-edge* nodes to provide a certain level of latency nationwide and facilitate the hosting of an initial wave of less latency-demanding edge applications, including telecommunication network functions like some 5G core components, the virtual RAN central units, or the transport SDN controllers. |
| *Short/mid-term* | The *user plane* will have to *be selectively extended to the far-edge* nodes to cope with ultra-low latency or very local residency demands, until the main verticals and demand areas are covered. |
| *Short/mid-term* | The architecture of the IP network will have to be optimised, reducing the number of hops between any two endpoints by limiting the levels in the hierarchy to a reasonable number, four to five, as shown in the figure. The latter is expected to contribute to improved latency and economic efficiency. |

# Focus area: End-to-end networking for the Edge-to-Cloud Continuum

Many applications from different domains / sectors will not reside just at the edge or in the cloud but will have service components deployed in both types of computing nodes, which will need to be properly chained (i.e. connected). A performing, dynamic, and scalable connectivity among the different nodes in the edge-to-cloud continuum will be thus be needed, occasionally requiring the participation of different communication service providers when the nodes hosting the components are located in different networks.

## 7.4. Technology Priority: Sustainable Transport Technology to Connect Edge-to-Cloud

#### Key drivers

Network traffic grows 30-50% yearly, but new edge-demanding applications like the Metaverse may require a 20x increase in traffic in the next decade [120]. The transport network needs to be adapted not just at topology level, to reduce the number of hops required to connect any two endpoints, but also needs to incorporate new technology innovations that further reduce the cost per transferred byte, minimising resource and energy consumption.

In the transport network domain, automation is targeted by projects like MUST [121], also part of the TIP initiative, which needs to be further supported towards enhanced network programmability, while initiatives like OOPT [122] (Open Optical and Packet Transport) at TIP [123] (Telecom Infra Project) are highlighting requirements [124], specifications, and reference implementations of open and disaggregated transport solutions that are key for scalable and efficient alternative technologies.

### Dependencies

The proposed priority has no dependency on other technology or deployment priorities, but it is advisable to ensure this is well coordinated with deployment priority *0. 7.3. Deployment Priority: Deliver a Performing Device Connectivity to the* Edge, since the architecture, topology, and interfaces of the transport network need to be changed to introduce new more efficient, capable, and scalable transport technology.

### Relevant use cases / application domains

Transport efficiency is especially relevant for edge applications demanding a heavy traffic exchange between user and edge, or between edge or cloud nodes, like those based on video analytics or data-intensive machine learning/artificial intelligence requiring an intensive data-feed, as may be the case for *Smart City* or *Energy grid management* solutions.

In edge applications with user mobility, such as the *Vehicle Driving Assistance* or the *In-vehicle entertainment*, the application instances will have to "follow" the customer and the corresponding connectivity between edge and cloud may require adaptation as the concentration of served users at a certain edge node grows or declines, impacting the size of the edge applications' instances in the node and the amount of traffic the edge node needs to run. The automatic adaptation of the network to these changing needs will be essential to make the operation sustainable.

### *Recommendations*

| | |
|---|---|
| *Short/mid-term* | New, high-speed reconfigurable optical interfaces, in the form of pluggable devices, will allow deep integration with network and compute devices, lowering CAPEX by eliminating interconnecting devices such as transponders, with benefits also in terms of OPEX by reducing card inventory, simplifying ordering, and saving power. Interoperable interfaces both in terms of optical performance and modelling would break vendor lock-in and further lower overall transport cost. Especially for edge nodes' connectivity towards the core, when distances are not too large and fibre may be a scarce resource, bi-directional pluggable optical interfaces used together with passive optical multiplexing technologies would be advisable to further reduce power consumption and CAPEX. |
| *Mid-term* | In the transport network domain, automation will be a major theme by reducing / eliminating manual interactions and speeding up operation processes. Automation |

should be enabled by creating a flexible overlay networking on top on the transport, allowing easy programmability of the network. The utilisation of Software Defined Network (SDN) principles, the separation of the data and control planes, and the openness and disaggregation will facilitate this automation. E2E network slicing [112] capabilities, including the connectivity of computing nodes across the transport network domain, need to be developed and progressively introduced in the communication networks supporting the edge-to-cloud continuum.

## 7.5. Deployment Priority: Sustainable Transport Network Transformation to cover Edge and Cloud Traffic Demand

### Key drivers

Video traffic grows by 30% year on year. New immersive content (e.g. AR/VR, 360 video, etc.) will further increase this growth to up to 20x over the next decade [120] with TV and video tripling average home monthly Internet usage to beyond 1 TB by 2025 [125]. New designs need to be developed, integrated, and tested before moving to a massive transformation. Its optimisation will be a key factor for the development of edge at scale.

Additionally, the number of network elements to replace, relocate, or reconfigure is significant, and the change will require time and effort. This change must be made gradually following the evolution of demand at near and far edge nodes, as also described in *7.3. Deployment Priority: Deliver a Performing Device Connectivity to the* Edge.

### Dependencies

This deployment challenge complements the efficiency in the access network covered by the *7.3. Deployment Priority: Deliver a Performing Device Connectivity to the* Edge, providing a sustainable transport of information between nodes in the edge-to-cloud continuum, necessary in applications that will have some service components in different nodes that need to be chained (connected) to exchange information.

On the other hand, the transformation of the transport network will trigger the replacement of legacy technology by more capable, scalable, and flexible alternatives like the one developed in *7.4. Technology Priority: Sustainable Transport Technology to Connect* Edge-to-Cloud.

### Relevant use cases / application domains

In edge solutions that automate business processes by applying a data-driven strategy, it is quite common to have a solution architecture that implements some parts of the processing in the cloud and other parts at the edge. In this type of application, a service function chain is required to connect the modules in the different computing nodes based on a quality and efficient underlying

connectivity. For instance, in systems controlling vast amounts of elements, like *Logistics and Warehousing* or *Industrial IoT*, the amount of data generated that requires processing is huge. It is common to pre-process and curate it close to the source (at the edge) and send only clean data to the cloud, where analytics and algorithms are applied to create models that contribute to the optimisation and automation of the processing. These models are downloaded from the cloud to the edge nodes.

The same applies for *video surveillance systems* in which the video monitoring and analysis is made at the edge and when anomalies are detected, images are sent to a central cloud module that coordinates the response to the incidence, triggering the corresponding actions.

In all these cases, the transfer of data between edge and cloud is significant and constant, and data transport needs to be optimised.

### *Recommendations*

| | |
|---|---|
| *Short-term* | The optimisation should start by upgrading the connection between near-edge nodes and the cloud infrastructure with more efficient and scalable technology. This corresponds to the transit and interconnection levels as shown in Figure 21: Edge connectivity to fixed and mobile access networks. |
| *Short/mid-term* | The upgrade should happen on demand and more progressively in the connection of the far-edge nodes with the near-edge and cloud. This corresponds to the service level as shown in Figure 21: Edge connectivity to fixed and mobile access networks. |
| *Mid-term* | Towards efficient scalability for edge computing, the automation and orchestration mechanisms defined in *7.4. Technology Priority: Sustainable Transport Technology to Connect* Edge-to-Cloud need to be implemented. It will require adding an abstraction and control layer in all network domains (access, transport, core), implementing the network orchestration on top, and coordinating it with the multi-cloud orchestration. It represents a paramount effort that will take significant time. |

## 7.6. Deployment Priority: Deploying the Right Infrastructure to Interconnect Service Providers

#### Key drivers

The connectivity providers should deliver timely access to innovative infrastructure resources that support adaptive, resilient, secure, and compliant digital business models. In this context, support will be given for a digital transformation by means of an agile, resilient, and distributed approach that requires mastering connectivity with proper performance and availability, network bandwidth,

and resiliency, in a multi-provider environment. Several properties need to considered, including: (i) *location identification* in terms of usage since interconnectivity was a primary factor in peering and content delivery networks (CDNs), and results suggest that edge computing selection could be the same, (ii) *security by design* (i.e. data inside EU, traffic exchanged in EU-only network) since layer 1 encryption will only address in-flight data and, thus, is only part of a security solution, (iii) *flexibility* to allow adaptation to changing business needs and environmental forces at agile software speed, (iv) *simplicity* to avoid ingress barrier and slow-rate adoption, (v) *performance* as latency and throughput, with an intrinsic *reliability* leveraging future technology evolution (i.e. 400/800GBit/s rates exploited), (vi) *scalability* accordingly to the business demands and market uptake, providing fast delivery and time-to-market, and (vii) *automation and orchestration*, creating interconnection at business speed (e.g. X-Connect creation in data centre, L2/L3 segment context creation, etc.).

### Dependencies

Technologies developed in the *7.4. Technology Priority: Sustainable Transport Technology to Connect* Edge-to-Cloud will also be applicable to the interconnection of networks from different providers, not just those associated with efficiency (open, disaggregated solutions) but also the ones related to automation and orchestration (SDN and network slicing).

### Relevant use cases / application domains

Many verticals, like the *automotive* industry, require connectivity to be supported across different market and operator networks, as the connected device, the vehicle, moves across different geographies.

Moreover, and due to its sensitivity to latency, applications like *assisted-driving* need to be delivered from a point close to the vehicle, whatever is its location or the network it is connected to.

## *Recommendations*

| | |
|---|---|
| *Short/mid-term* | Interconnection among network service providers will have to be upgraded to higher capacity and resiliency, using efficient transport technologies. The interconnection and roaming agreements will have to be reviewed to serve the new edge applications. |
| *Mid-term* | Automation and orchestration mechanisms defined in *7.4. Technology Priority: Sustainable Transport Technology to Connect* Edge-to-Cloud (SDN, Network Slicing) need to be implemented, including federation interfaces to facilitate an automatic and dynamic interconnection among operators. |

# Focus area: Achieving scale at the Edge by hosting Telco Network Functions

5G is being rolled out at high speed in the US and Asia, with Europe still lagging behind [103]. In 2021, 4% of the mobile traffic ran on 5G networks in Europe, while 5G represented 13% of the total mobile traffic in US and 29% in China. The forecast for 2025 indicates Europe will reach 44% in 5G traffic penetration, well below US and China with 63% and 52% respectively, but also below Arab States and the Developed Asia Pacific, with 49% and 64% respectively.

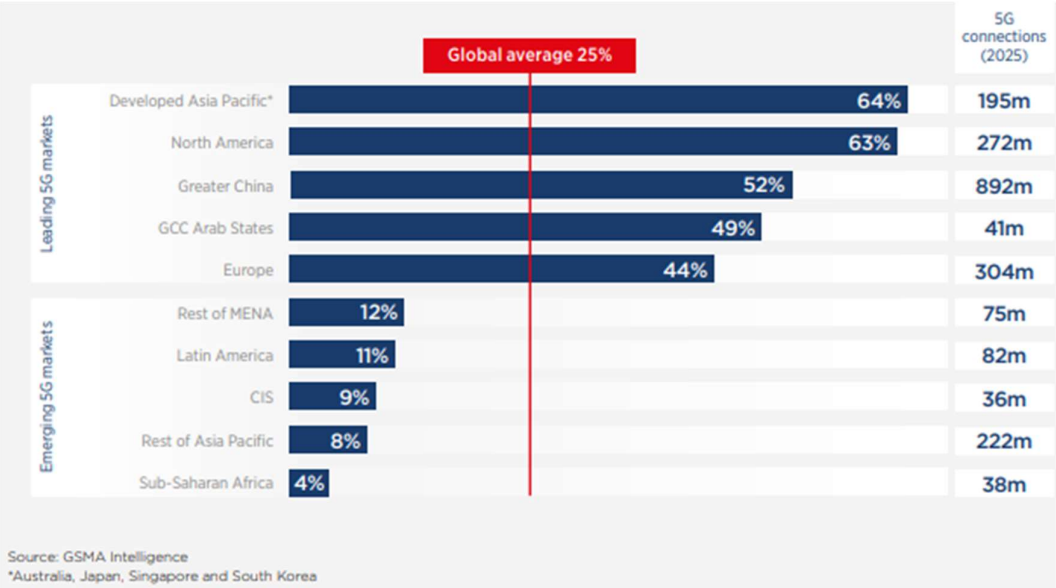



*Figure 23: 5G markets and connections worldwide (Source: GSMA Intelligence)*

To take the lead in the digitalisation era, Europe needs to ensure that the platform for innovation built by ubiquitous advanced 5G and fibre access networks and their exposed capabilities, high-capacity fibre interconnectivity, and the distributed cloud resources evolves in a coordinated way. The combination of all these capabilities, rather than each element in isolation, will ensure the competitiveness of the European industry. In fact, if the edge-to-cloud continuum is designed properly and deployed in a timely manner, it may host the 5G and fibre-to-the-home network functions and benefit from the scale of the European telecom industry.

The *disaggregation of hardware and software* in radio access network functions offers cloud service providers the opportunity to provision commodity computing nodes at the edge data centre that can be used to host accelerated cloud-based RAN software for multiple operators.

What is more, the *centralisation of computationally intensive tasks* at edge data centres (e.g. 5G baseband processing) enables pooling gains through elasticity of the edge cloud and through consolidation of Enterprise and 5G (RAN) workloads, resulting in greater energy efficiency and reduced carbon footprint.

## 7.7. Technology Priority: Network Functions as a Main Tenant at the Edge

### Key drivers

To provide the level scale desired for edge services, network function themselves need to represent a tenant of the edge deployment and be deployed / distributed across edge and cloud environments, including on-premise edge, network-access edge, network- core edge, and cloud data centres, as depicted in the figure.

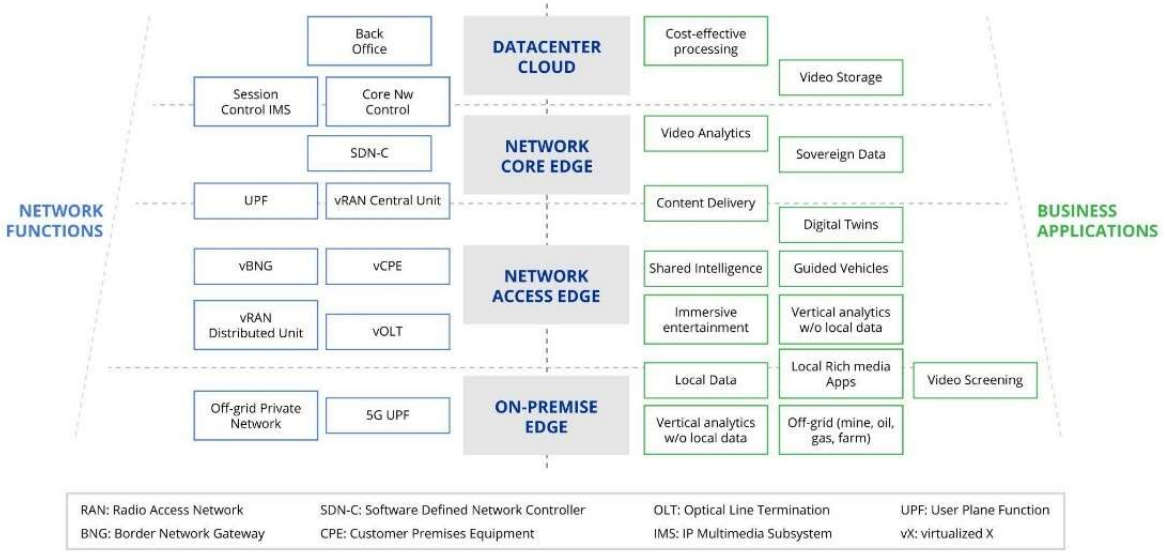



*Figure 24: Distribution of network technology across edge and cloud environments*

### Dependencies

This topic depends on all the other technology priorities to enable an adequate edge-cloud computing framework that can properly host the telecom network functions, meeting the performance and security requirements of these services and critical infrastructure:

*1.1. Technology Priority: Representation in Open Standards, Relation to Norms &* Standards*:* Telecommunications are critical services that require business continuity. To achieve this, the Telco Industry needs diversity of supply, that is, the chance to easily swap a technology with an alternative one in case it fails in short time. Several companies need to provide compatible, interoperable, and interconnectable technologies. Open standards and reference implementations facilitate this.

*2.6.* Technology Priority: Support Distributed & Interoperable Architectures*:* Decentralised architectures with distributed data processing and storage should be promoted in the short term, further expanding the capillarity of edge infrastructure, covering the coverage, capacity, performance, interoperability, compatibility, and portability requirements of Telco network functions across all geographies.

*3.1. Technology Priority: Sustainability by* Design*:* The European standards for sustainable software development should be also applicable to telecom network functions.

*4.1. Technology Priority: EU innovative Data Encryption Technologies including Quantum-safe & Privacy-enhancing* Encryptions*:* For the adoption of edge computing in verticals with highly sensitive data, like the telecom sector, data security and privacy need to be preserved. Technologies like quantum safe encryption will also be required for the Telco sector.

*5.1. Technology Priority: Open Standards for Cloud Infrastructure* Services*:* These are necessary to facilitate the usage and management of the heterogeneous, hybrid multi-cloud environments that networks require.

*5.2. Technology Priority: Uniform Abstraction Layer for Multi-provider* Portability*:* Networks will run over a hybrid multi-cloud environment. This abstraction layer will facilitate the deployment, operation, and management in this environment.

*5.3. Technology Priority: Multi-provider Meta-Orchestration and Workload* Optimisation*:* Communication service providers may benefit from having a single / unified management interface to manage and deploy resources (i.e. network functions) on different cloud environments.5.4. Technology Priority: Multi-provider Edge Cloud Federation*:* For scenarios in which a network function needs to be deployed beyond its footprint, edge cloud federation may be necessary.

*8.1. Technology Priority: Establish an Open Hardware* Ecosystem*:* The Telco industry may benefit from the use of open hardware. Until now, network technology has been based on proprietary network appliances.

*8.5. Technology Priority: Adapting and Improving Operating* Systems*:* General purpose cloud stack software needs to be adapted and extended to provide a carrier-grade environment for the execution of network functions.

*Focus area: Edge-to-Cloud Service Life Cycle Management:* The availability of open and standard cloud and edge stacks, through compatible and interoperable commercial platform distributions, will greatly help the supply diversity and business continuity of telecom networks. These tools can also help telecom operators in the management of complex CNF-based network configurations, providing automation and flexibility in network deployment and operation.

### Relevant use cases / application domains

Given the scope of this priority, the respective use cases are relevant to the network functions and applicable by default, enabling the edge-to-cloud continuum to host both the industry and telecommunication use cases. Thus, focus is put on the network functions, most of which will be migrated over time to a cloud-native software-based format. These are: (i) fibre-to-the-home network functions, including the optical line termination, the border network gateway / broadband remote access server, (ii) virtualised radio access network functions, both central and distributed units, (iii) virtual customer premises equipment, (iv) 5G core network functions, both control and

user planes, and, in the future, 6G, (v) other control elements, like the SDN-C (Software Defined Network Controllers) of the transport network or the IMS (IP Multimedia Subsystem, that controls multimedia communication sessions), (vi) private networks for on-premises deployments, and (vii) other over-the-top connectivity services like firewalls, SD-WAN (Software-Defined Wide Area Networks), etc.

### *Recommendations*

| | |
|---|---|
| *Short/mid-term* | *Edge cybersecurity* must be built to ensure trusted architecture in collaborative edge. This includes a new network security model that combines multiple controls such as Zero Trust Network Access (ZTNA), Cloud Access Security Broker (CASB), firewall as a service (FWaaS), or data loss protection (DLP). |
| *Short/mid-term* | *Network-as-a-Service APIs*, supported by Software-Defined Networking technology, will provide the means for automatic dynamic bandwidth allocation and latency configuration, optimising resource utilisation. |
| *Short/mid-term* | For some network functions (e.g. user plane functions like the Core UPF or vRAN units) the *cloud environments* should be able to *scale down to smaller environments* with limited hardware resources and power availability. |
| *Short/mid-term* | Many 5G network functions run well on off-the-shelf platforms, but as bandwidth increases and advanced antenna systems are deployed, off-the-shelf hardware cannot keep up and drives high levels of power consumption. *Hardware acceleration* is needed for the compute-heavy physical layer and scheduling workloads in 5G, possibly attained using GPUs, FPGAs, or ASICs. |
| *Mid-term* | *Multi-vendor orchestration and assurance* mechanisms will be required. These should be agnostic to the edge infrastructure, be able to bring together and orchestrate applications and services across network domains including the edge-cloud infrastructure, and ensure the required SLAs (see Section 5 and Section 9). These mechanisms should provide the necessary automation level to manage the complexity of the hybrid multi-cloud Telco environment and dynamically distribute the different network functions. |

## 7.8. Deployment Priority: Edge Infrastructure Deployment to support the Network Evolution to Cloud-native

#### Key drivers

The European mobile network, with its widely distributed architecture, must evolve to adopt 5G and become cloud native, enabling industry and telecommunication use cases. There is a unique opportunity to leverage both the strength of European telecom vendors [127], who are globally

leading in providing cloud native 5G, but also the global footprint of European telecom operators [128]. These combined strengths can form the basis for a compelling value proposition in cloud edge, realised by transforming the mobile network into a network of widely distributed cloud edge nodes, implemented on standards-based cloud technology and open source components, but also by highlighting telecom technologies that offer *distributed high-performance computing*, higher bandwidths, lower latency, and higher resilience, regardless of the physical location of the device.

Cloud technology standards and edge infrastructure will both have to evolve at the right speed and to the right extent to provide a proper *environment for the execution of the functions supporting the new network generations* (e.g. 5G/6G, FTTH/50GPON, WiFi6/7, etc.). Moreover, networks will require a timely deployment of a distributed edge infrastructure to host the network functions from the different domains (access, transport, core).

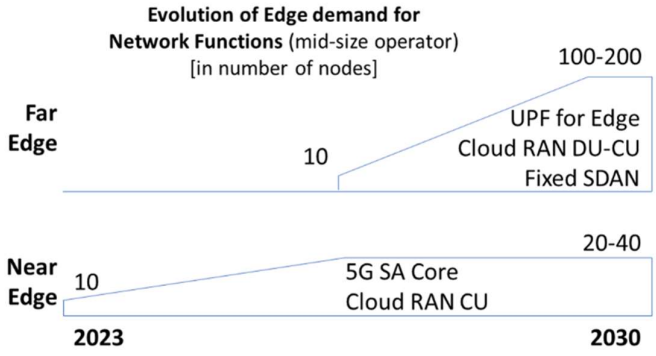



*Figure 25: Network Function demand of Edge nodes in a typical mid-size telecom operator*

### Dependencies

This topic depends on all the other technology priorities to enable an adequate edge-cloud computing framework that can properly host the telecom network functions, meeting the performance and security requirements of these critical infrastructure and services. For a detailed list of dependencies please refer to the Dependencies subsection related to the Technology Priority: Network Functions as a main tenant at the Edge.

### Relevant use cases / application domains

Given the scope of this priority, the respective use cases are relevant to the ones listed in the Relevant use cases / application domains subsection related to the Technology Priority: Network Functions as a main tenant at the edge.

***Recommendations***

| | |
|---|---|
| *Short-term* | Implement the 5G SA Core at near-edge nodes, enabling them to serve business applications as well and to provide a uniform edge experience market-wide. User plane functions will be installed in all nodes to provide the required local breakout in the corresponding service area. |
| *Short/mid-term* | Initiate the virtualisation of the radio access networks by installing vCUs (virtualised Central Units, control elements of the RAN) at the near-edge nodes and selectively deploying far-edge nodes to meet demand from first vDUs (virtualised Distributed Units, baseband processing elements of the RAN) and first virtualised OLTs (vOLTs). Start the distribution of small UPFs in each far-edge node. |
| *Mid/long-term* | Complete the virtualisation of the radio access network (complete set of vDUs) and the fibre access network (i.e. vOLT and vBNGs - Border Network Gateways) at far-edge nodes to move towards a final footprint that can serve ultra-low latency and ultra-reliable edge applications. |

## 7.9. Deployment Priority: Coordination of Network Orchestration with Multi-cloud Orchestration

### Key drivers

*Network slicing* will allow certain edge applications to be provided with a dedicated logical network that meets their connectivity requirements. Slicing requires the deployment, activation, and orchestration of certain network resources in the access, transport, and core network domains to deliver the necessary characteristics.

*Slice orchestration* should be highly automated and supported by an adequate level of abstraction of each resource domain. Abstraction simplifies the resource details (such as quantity, vendors, location of the resource, physical details, real topology and so on) and transforms them into digital assets that can be managed using software by the network orchestrator. By logically separating the service from the infrastructure technologies, the abstraction technique makes services independent from the underlying network and cloud resources, allowing these two elements to evolve independently. As an example, a network service could be constituted by a chain of network functions. Transport provides the connectivity among them. One of the main challenges is the optimisation of resource placement on top of the underlying transport infrastructure. For example, network functions can be connected through a simple point-to-point transport link or, alternatively, through a meshed geographical transport network. These two options imply different latency values or different availability. Knowledge of transport characteristics is particularly relevant in the case of services with critical performance requirements.

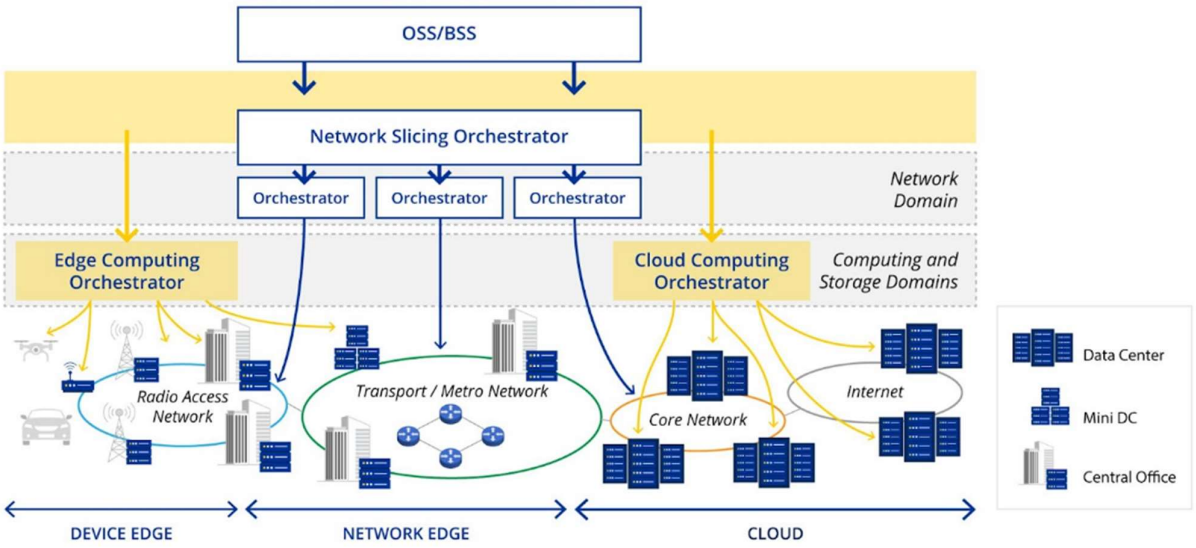



*Figure 26: Coordination of network orchestration and cloud orchestration*

The *network slice orchestration relies on the multi-cloud orchestration* to deploy and automatically scale up / down the required network resource capacity (i.e. network functions) in the most optimal location. On the other hand, many applications will have software modules distributed across the edge-to-cloud continuum that need to be properly connected. *Multi-cloud orchestration* oversees the placing of each module in the most optimal cloud or edge environment and *relies on the network orchestration* to provide the connectivity between the modules to deliver the right performance and application experience.

### Dependencies

*5.2. Technology Priority: Uniform Abstraction Layer for Multi-provider* Portability*:* Networks will run over a hybrid multi-cloud environment. This abstraction layer will facilitate the deployment, operation, and management in this environment.

*5.3. Technology Priority: Multi-provider Meta-Orchestration and Workload* Optimisation*:* Communication service providers may benefit from having a unified management interface to manage and deploy resources (network functions) on different cloud environments.

*Focus area: Edge-to-Cloud Service Life Cycle Management:* These tools can help telecom operators in the management of complex CNF-based network configurations, providing automation and flexibility in network deployment and operation.

*7.4. Technology Priority: Sustainable Transport Technology to Connect* Edge-to-Cloud*:* The dynamic E2E network slicing automates the connectivity between related modules in a service chain, facilitating the orchestration of solutions across an edge-to-cloud continuum.

### Relevant use cases / application domains

Complex solutions combining software components in different types of computing nodes (e.g. on-premises, near edge, central cloud, etc.) will require a level of automation that only sophisticated systems combining network and cloud orchestration can deliver. This is typical in *video surveillance applications* that need to continuously process video images to identify incidents or anomalies (with video analytic functions in edge nodes), process them to take decisions, and send them to a central node for analytics, fine-tuning the models used for inference and updating them in the local nodes.

### *Recommendations*

| | |
|---|---|
| *Mid-term* | Slice orchestration should be highly automated and supported by an adequate level of abstraction of each resource domain. It will rely on the multi-cloud orchestration to automatically deploy and scale up and down the required network resource capacity. On the other hand, multi-cloud orchestration will use the network orchestration mechanisms to dynamically connect the different edge and cloud nodes. |

# SECTION 8: CLOUD - EDGE FOUNDATION INFRASTRUCTURE

This section addresses the complete infrastructure that is needed for edge, cloud, or edge-to-cloud continuum. It does not only cover the physical devices and cabling that are needed to run cloud services, like servers, switches, and routers as well as the management platform that is needed to run, operate, and monitor them, including a first layer of orchestration. The section also covers the infrastructure needed to establish a highly secure and open environment in which an edge-to-cloud continuum can be developed and implemented. This edge-to-cloud continuum infrastructure will facilitate: (i) *dynamic workloads*, incorporating servers / switches for a wide range of workloads and enabling the dynamic utilisation of servers / switches and edge sites, (ii) *different types of workloads*, triggering an overall infrastructure design / architecture such as switches that can run workloads or a server with embedded switches, (iii) *handling of data that need to be protected* through special-purpose hardware (e.g. CPUs) and software (e.g. confidential computing or TEE), (iv) *special hardware provisioning* (e.g. GPUs, ASICs, FPGAs) since this is required by some applications which need special hardware, (v) *workload resource usage interface specification*, through interfaces enabling us to define which infrastructure is usable and which resources need to be used, (vi) *high-availability and disaster recovery*, accomplished both by design (efficient packaging to minimise failure) and by supporting dynamic reallocation of resources from faulty to working resources, (vii) *a wide and common set of metrics and telemetry*, facilitating guaranteed QoS along the edge-to-cloud continuum, as well as optimisation of energy consumption through a vertical flow of control information between application and service layers, and (viii) *knowledge and technologies for edge-to-cloud continuum establishment and know-how*.

In this context, this section includes recommendations to establish a research and development infrastructure needed to implement an edge-to-cloud continuum. As this is a very wide and complex area, the current section focuses on a small selection of topics which are seen as the most important. The goal is to provide a base for a federation and application layer by making use of the infrastructure and networking. In addition, the cross-functional topics like base technologies such as encryption, security, or sovereignty are considered.

Deployments range from central data centres, near and far edge nodes, customer, and service provider on-premises installations. This is accompanied by a high variance in optimisation capabilities, specialisation, physical space, power and cooling limitations, and rough environments for far edges. Some use cases might require special hardware like FPGAs, high throughput NICs, and PHCs which are able to handle PTP, GPUs, and ASICs. These factors and the resulting requirements include edge node hardware design, BMC, firmware and BIOS / UEFI usage, upgrades and configuration, operating system, resource abstraction such as containers or serverless computing, and cloud orchestration and management for compute, storage, and network.

Currently the market and the technologies described above are controlled by non-European companies and industry standards [129], [130]. In order for Europe to become more independent and self-sufficient in the future, efforts are required on a technological as well as on an organisational and intellectual property level.

## Focus area: Establish EU Ecosystem for Open Hardware

Open hardware refers to hardware designs that are made publicly available and can be freely used, modified, and distributed by anyone. Overall, open hardware offers a number of advantages over legacy hardware, including promoting innovation and collaboration, being cost-effective, transparent and accountable, and being more sustainable.

Open hardware promotes innovation and collaboration. By making hardware designs publicly available, designers and developers can build upon and improve existing designs, leading to a faster pace of innovation. Open hardware also enables more people to participate in the development process, which can lead to a greater diversity of ideas and solutions. Another advantage of open hardware is that it is often more cost-effective than proprietary hardware. Because open hardware designs can be freely used and modified, users do not have to pay for licenses or royalty fees. This can make it more affordable for individuals and organisations to access and use hardware. Open hardware is also more transparent and accountable than proprietary hardware. Because the designs are publicly available, users can see how the hardware works and can verify that it meets their needs and standards. This can be especially important in situations where hardware is being used for critical or sensitive applications, such as in healthcare or government. Finally, open hardware can be more sustainable and environmentally friendly than proprietary hardware. Because open hardware designs can be freely shared and modified, users are less likely to throw away old hardware and replace it with new, proprietary hardware. This can reduce the environmental impact of hardware production and disposal.

One area where open hardware has made significant progress is in the development of open hardware micro-controllers, such as the Arduino [131] and Raspberry Pi [132]. These micro-controllers have become popular for a wide range of applications from hobby projects to industrial control systems.

Furthermore, in the area of (central) data centres there has been a lot progress during recent years. Organisations like open19 [133] or TIP (Telecom Infra Project) [134] define standards which are implemented by hardware vendors [135].

There has also been a trend towards open hardware in the Internet of Things (IoT) space, with a number of open source hardware platforms and tools being developed for IoT applications. These platforms and tools enable developers to build and deploy IoT systems using open source hardware and software, allowing for greater customisation and flexibility.

Overall, the current state of the art of open hardware is marked by a growing number of open source hardware designs and tools, as well as a growing community of developers and users. While there are still challenges to be addressed such as intellectual property issues and the need for robust supply chains, the future of open hardware looks bright as it continues to gain traction and impact.

## 8.1. Technology Priority: Establish an Open Hardware Ecosystem

### Key drivers

Establishing an open hardware ecosystem is a complex process and therefore needs careful planning and the right approach to be successful. The main steps that can be taken to establish an open hardware ecosystem where start-up financing might act as a crystallization point are the following: (i) *identify the need and demand* for open hardware in order to assess the level of demand for open hardware and to specify which hardware is needed, (ii) *define the goals and vision* for the ecosystem, including setting of objectives such as promoting innovation, increasing collaboration, reducing costs, or improving sustainability, (iii) *identify potential stakeholders* (such as manufacturers, designers, developers, and users), to ensure that their needs and interests are taken into account, (iv) *develop a business model* to define how the ecosystem will generate revenue and sustain itself over time, including revenue streams (e.g. product sales, licensing, consulting, or training) and evaluate whether there is a need for a start-up financing, (v) *build a community of stakeholders* through activities such as online forums, hosting events and workshops, and engaging with stakeholders through social media and other channels, (vi) *develop and launch products and services* that meet the needs and interests of stakeholders, including hardware designs, software tools, and other resources that support the development and use of open hardware, (vii) *continuously improve and evolve the ecosystem* to meet the changing needs and expectations of stakeholders, through regular updates and improvements, as well as further engagement with stakeholders to gather feedback and ideas for future developments.

Developing, exchanging concepts and improving open hardware creates advantages for all participants. A start-up financing can push the infrastructure and ecosystem to a point where it is self-sustained. There are currently solutions available on different levels. open19 [133] and TIP (Telecom Infra Project) [134] partially define and standardise data centre equipment including cabling, and RISC-V [136] is an open standard instruction set architecture. Moreover, there are many companies that can create PCBs in a short period of time. In addition, there are PCB printers available that can print PCBs directly [138]. Besides the aforementioned solutions, there are also several current projects such as the “Open Source Hardware for Science and Beyond” [139] or “White Rabbit” [140] from CERN. Google provides a service to build silicon for free and provides the complete development tool chain including documentation [141]. A new project that was founded recently is *Balthazar:* an all-European RISC-V Free Hardware computer [137].

### Relevant use cases / application domains

As this contributes to every aspect of the infrastructure, all edge, cloud, and edge-to-cloud continuum use cases are relevant. Use cases that need high reliability, mobility, and security will profit most, e.g. healthcare, mobility, telecommunications, and AI.

This technology priority can be seen as one additional building block for *Resilient Infrastructure*, as described in HORIZON-CL3-2023 [150]. Relying on non-EU hardware with possible hidden security threats might render critical EU infrastructure vulnerable. Because this priority focuses on creation of autonomy and resilience in the EU, it expands the topic *Increased Autonomy in Key Strategic Value Chains for Resilient Industry* [151].

### *Recommendations*

| | |
|---|---|
| *Short-term* | As the current mainline hardware (including CPUs) uses closed source firmware (software) there is the need for some edge-to-cloud continuum use cases to have either a hardware build that does not use firmware at all or runs open-source firmware. EU to implement actions for the establishment of connections between different industry partners and research institutes (universities) to define and implement steps needed to create a complete hardware and firmware for an edge-to-cloud continuum stack in the EU. |
| *Mid-term* | As especially IoT and (handheld) edge devices typically do not need that much compute power, memory, or storage, there is therefore no need for the latest and fastest CPUs for these use cases. Edge and IoT devices can be designed to have exactly the functionality which is needed. This saves energy and dramatically minimises possible attack vectors. |
| *Mid/long-term* | EU to implement actions to utilise IT equipment, including regular updates and improvements to stay up-to-date and fulfil the latest requirements based on possible new use cases. |

## 8.2. Technology Priority: Print-And-Go, Implement Local Manufacturing for IT Equipment

### Key drivers

As the expected edge locations and use cases for the edge-to-cloud continuum might vary dramatically, specially adapted equipment is a solution: the hardware can be customised and manufactured specifically for each use case and / or edge location.

With the advent of 3D printers and small CNC machines, production is shifting more and more from large industries to places where the products are really needed. This has the advantage that goods that are precisely tailored to requirements can be manufactured directly on site [142]. In

addition, local manufacturing of Printed Circuit Boards (PCBs) and other IT hardware equipment can bring a number of advantages including: (i) *reduced transportation costs* and the corresponding *environmental impact* of transporting goods over long distances, which is particularly important for large and heavy items such as IT hardware, (ii) *improved supply chain resilience* by reducing reliance on overseas suppliers, contributing to the mitigation of the risk of disruptions caused by natural disasters, trade disputes, or other factors, (iii) *increased employment and economic development* by stimulating economic development in the local community, (iv) *enhanced security and privacy* as it reduces the risk of data breaches or unauthorised access during transportation or storage, which is of major importance for hardware used in sensitive applications such as government or healthcare-related settings, (v) *customisation and flexibility* in the design and production of IT hardware, enabling companies to efficiently meet specific customer requirements or make changes to their products as needed, (vi) *quality control* as it enables manufacturers to more easily monitor and address any issues that may arise during the production process.

### Dependencies

Availability of open source hardware models including software for easy customisation.

Because this priority focuses on creation of autonomy and resilience in the EU, it expands the topic *Increased Autonomy in Key Strategic Value Chains for Resilient Industry* [151].

### Relevant use cases / application domains

Several use cases could benefit from the proposed recommendations, with an emphasis on the ones that utilise small equipment or devices with limited high-reliability properties. For example, in the *next-gen engagement & human centricity* use case it is possible to create devices especially for individual uses and sizes. In the *technology – infrastructure providers: edge-to-cloud continuum* use case, the print-and-go approach supports solutions like swarm robotics that relay on many devices but with limited self-management capabilities.

The introduction of print-and-go approach will also considerably affect the *digital supply chain* use case because the supply chains will become much simpler as the product is created where it is used. As the equipment is built directly where it is used there is no need for transport, or only very limited transport is needed. Moreover, there is no need for warehousing or ordering possible further units as these are used.

## *Recommendations*

| | |
|---|---|
| *Short-term* | EU to implement actions to establish connections between different industry partners and research institutes (universities) to define and implement steps needed to create the infrastructure needed for local manufacturing. |

| | |
|---|---|
| *Mid/long-term* | EU to implement actions for utilising IT equipment, including regular updates and improvements to stay up-to-date and fulfil the latest requirements based on possible new use cases. |

## Focus area: Prepare and Optimise for Multi-Provider Multi-Cloud Environment

Current approaches for cluster management enable the handling of one cloud instance – sometimes only from the same vendor [143]. For sharing data and even workloads through a cloud continuum, there is a need for coordination between different vendors or cloud providers. There are standardised interfaces and APIs required to implement these features. As of now, the cost must be considered: while inbound traffic is typically free, outbound traffic generates costs, which adds complexity when transferring data or workloads from one cloud to another.

Moreover, cluster management typically lacks features for running and prioritising different workloads (e.g., low-latency-computing vs. batch jobs) – especially when it comes to external properties like different power consumption costs in different sites at different times.

Currently the management systems are optimised for (central) data centres, which means that it is assumed that there is always good connection. An EU-wide edge-to-cloud continuum introduces a new set of challenges such as managing partial network outages during which both the control and data plane are not reachable at all or only with limited bandwidth or high latency.

The provision of federated services is enabled by various mechanisms and interfaces: (i) the *east and westbound APIs*, tackled in Focus area: Orchestration and Federation of Distributed Edge Cloud, needed for the communication between different infrastructure providers and provision of services across providers, including data or workload move from one infrastructure (e.g. cloud) to another, handling of security aspects (like encryption during transfer), methods of adding or removing infrastructure providers, handling of service requests which utilise more than one infrastructure provider (e.g. reserving communication bandwidth using two endpoints which are under control of different infrastructure providers), and billing, and (ii) the northbound API, tackled in Section 9: Infrastructure and Platform Services, which facilitates the provision of the services through a single provider.

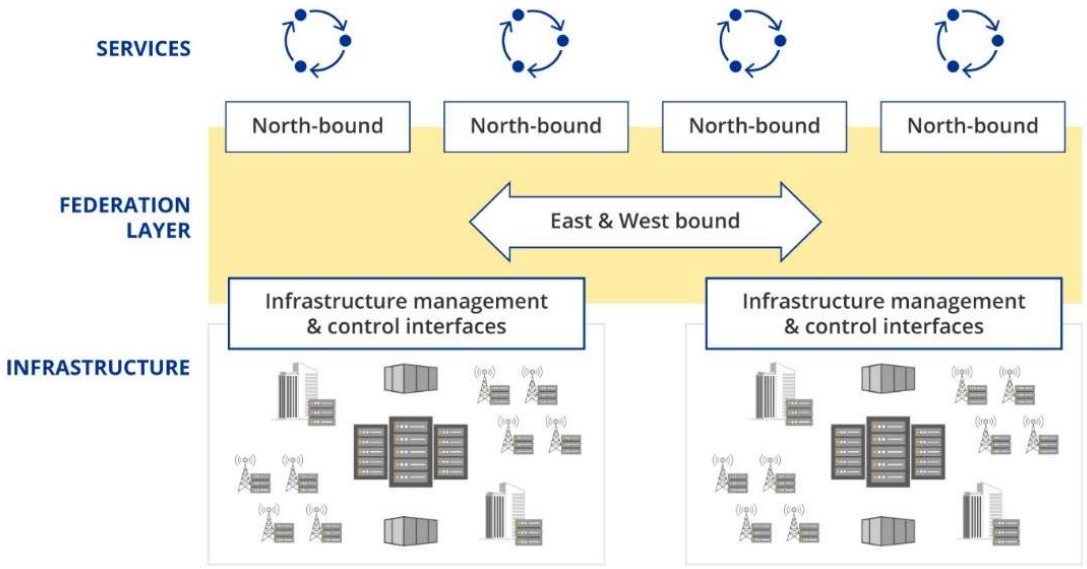



*Figure 27: Federation Layer API utilizing infrastructure from different providers*

In order for the federation to be realised, relevant information needs to be obtained from the infrastructure and according to federation decisions trigger the appropriate actions (i.e. control). The current section tackles the latter through these interfaces, the *infrastructure management & control interfaces*, enabling inventory handling (i.e. which resources are available), reservation, usage, monitoring, maintenance, operations, etc.

## 8.3. Technology Priority: Implement Security from Ground up, Inherent in Every Aspect of the Infrastructure

### Key drivers

One central goal of establishing a multi-provider cloud is to be able to move workloads and data between clouds from different infrastructure providers or to access data on an infrastructure from a different infrastructure provider. Depending on the service, a workload might be started on a cloud from another cloud provider or might be moved to it. These use cases introduce a complete new set of requirements for the infrastructure as the data must be handled in such a way that none of the included infrastructure providers is able to read the data. This is true for storing, transferring, and processing the data or the application. However, as not all application and data falls under the same level of confidentiality it makes sense to create a set of predefined confidentiality levels, e.g. public, confidential, personal. If the level is not available or if an element of the infrastructure was compromised, precautions must be implemented, like notifying the application or immediately deleting all workloads and data.

Additionally, in an edge-to-cloud continuum scenario not all infrastructure can be placed in well secured buildings or places. Depending on the location of an edge device, many untrustworthy people might have access to it. Therefore, there is the need to implement measures to handle attack attempts on all levels, such as network attack or direct physical access. Using perimeter defence will not be possible in an edge-to-cloud continuum; instead, technologies like ZeroTrust might be used.

Nowadays, several functionalities of even typical hardware devices, like NICs or CPUs, are built using software [144]. To be able to build a complete trustworthy stack each and every component of the infrastructure needs to use open source, well designed, and verified software on all layers. Symmetric and asymmetric algorithms for encryption and decryption are also required to encrypt the data when stored, transferred, or processed. Two examples of well-known algorithms or libraries are openssl [145] and AES [146]. AMD Memory Encryption [147] is a solution that enables data encryption while stored in RAM. Google Cloud provides a product that uses a TEE (Trusted Execution Environment) to implement Confidential Computing [148], while other cloud providers offer similar products. None of the algorithms, libraries, hardware, or services are (completely) open source. None of them can be completely trusted because quantum computers are just within reach and could break a lot of currently used encryption, so there might be a need to develop new encryption algorithms.

#### Relevant use cases / application domains

Security is a basic layer when it comes to many use cases - especially if they need to handle private data which falls under the GDPR of the EU. As health data is very specific and personalised data with special protection according to the GDPR the *next-gen engagement & human centricity* use case is affected.

In addition, basic infrastructure elements such as the ones in the *telecom – mobile networks driving cloud edge* use case are affected, as they need to provide the base for the transfer of private data. For this use case there is the condition that the application data must not be read by the infrastructure provider, which requires technologies like TEE or Confidential Computing.

### *Recommendations*

| | |
|---|---|
| *Short-term* | Evaluate existing technologies in the field of security and cryptography requirements needed for an edge-to-cloud continuum. Focus on the new use cases like running workloads using personal data on unknown clouds or environments. Establish methods to check for a workload if the underlying infrastructure is compromised. Define levels of trustworthiness: not all workloads need the highest security policies. |
| *Mid/long-term* | Establish technology stacks starting from the ground (e.g. include CPUs, firmware, etc.) to implement the different levels of security policies. |

## 8.4. Technology Priority: Define and Implement the Infrastructure management & control interface

### Key drivers

A common interface is required for all aspects of the infrastructure providing the infrastructure-related information and enabling the corresponding utilisation of control-related decisions towards the infrastructure. These include inventory management (e.g. a list of infrastructure providers and details of the infrastructure of each provider, dynamic adoption of this infrastructure since it might be added, changed, or removed), infrastructure costs for different usage types and times, reservation of infrastructure, allocation, usage, and deallocation of infrastructure. The interface should be able to handle requests and trigger decisions based on several aspects such as availability and reliability (e.g. through a distributed management and monitoring system), dynamicity (enabling consideration of infrastructure changes), security (since not all workloads and data need the same security levels), quality of service (e.g. throughput, reliability, etc.), diversity in usage times (e.g. nights, weekends, energy costs etc.), diversity in usage types (e.g. immediately, batch, reservation, unreliable, etc.), and costs (e.g. cost of "1 CPU" unit).

Having a federation layer is a precondition for an EU wide edge-to-cloud continuum and the infrastructure and control interface is a core element in the scope of the federation. This builds upon existing projects like SNS-2022-STREAM-A-01-05: Edge Computing Evolution or SNS-2022-STREAM-A-01-06: Trustworthy and Reliable End-to-end connectivity Software platforms [152].

Currently each cloud provider focuses on its own infrastructure. There are approaches to "hide" infrastructure of other cloud providers beneath one's own API [153], but this is very limiting and does not solve the problem. Alternatively, there are standardisation organisations that have picked up this topic and are working on a federation API, but these are currently too limiting and are focused on one use case only. One example relates to the GSMA that had defined a federation API for edge service providers tackling various services [154].

### Dependencies

The northbound and southbound interfaces must be specified and developed in close collaboration with east and westbound interfaces of the federation layer, which are defined in the *Focus area: Orchestration and Federation of Distributed Edge Cloud*.

### Relevant use cases / application domains

Several use cases can utilise the proposed recommendations. A representative example refers to the *infrastructure –edge-to-cloud continuum* use case, since the definition of a management and control interface directly affects the use case, as this is the element where the API needs to be implemented.

### *Recommendations*

| | |
|---|---|
| *Short-term* | Definition of a federation API and its reference implementation. EU to implement actions to involve partners from different industries, public and health sectors as well as research institutes in order to define the edge-to-cloud continuum federation, to then define and implement a federation API. Each partner will provide a small lab set-up to interconnect with the others. As a first starting point the federation API can be implemented as an adapter using existing cloud management systems. The API should be based on well-defined use cases, make use of up-to-date technologies, and should be completely open source. |
| *Mid-term* | Develop partnership and collaborations with other organisations, industry and government partners. Establish procedures and organisations which can handle the challenge of a rapidly developing and changing technological ecosystem. Adapt and change the federation API according to the technological, environmental, and user needs. Native implementation of the federation API with special focus on security and privacy (e.g. move encrypted workload and data from a cloud of one infrastructure provider to a cloud of a different infrastructure provider and take care that the encryption stays intact during the complete hand-over procedure). |
| *Long-term* | Improve the implementation and adapt to new versions of the API. Establish a strong and diverse community of industry partners and developers as well as standardisation bodies to adapt to and implement the challenges and changes needed. Foster education and training for users as well as for developers of the API. |

## Focus area: Develop and Adapt Basic Software Components

Developing and adapting basic software components like operating systems, software for hardware operation, management, and monitoring is essential for cloud solutions to function effectively. These components are the base on which to offer a range of services such as virtual machines, storage, and networking, that can be accessed by users on demand.

Operating systems are the foundation of any computing platform and a cloud solution must have a robust and reliable operating system to ensure that services are delivered consistently and reliably. This includes the ability to handle multiple workloads simultaneously, as well as the ability to scale up or down as needed.

Hardware operation is also critical for cloud solutions as the provider must be able to effectively manage and maintain the underlying hardware infrastructure. This includes tasks such as

provisioning, monitoring, and maintenance of physical servers, storage devices, and networking equipment.

Software operation is another important aspect of cloud solutions, as it involves the management and maintenance of the software that runs on the cloud platform. This includes tasks such as patching and updating software, as well as monitoring and troubleshooting any issues that may arise.

Management and monitoring are key components of any cloud solution as they enable the provider to monitor the performance and availability of services, and to take corrective action if needed. This includes tasks such as monitoring resource usage, identifying potential issues, and implementing measures to prevent outages or downtime.

## 8.5. Technology Priority: Adapting and Improving Operating Systems

### Key drivers

More and more functionalities will move from the central data centres towards the edges and even on-premises. Because of the increasing number of use cases, the operating systems must implement different requirements, like low-latency computing for machine control or signal processing, or support for running AI/ML models on handheld devices.

In terms of security, a strong and secure operating system is essential for protecting the cloud and its users from external threats such as hackers and malware. This includes features such as encryption, authentication, and access controls to prevent unauthorised access to sensitive data and resources.

Reliability is another important consideration for operating systems in the cloud. Users rely on the cloud to access critical resources and services, and a reliable operating system is essential for ensuring that these services are available when needed. This includes features such as failover and backup mechanisms to prevent outages and downtime.

Privacy is also a key concern for operating systems in the cloud as users need to trust that their data will be protected and kept confidential. This includes measures such as data encryption and secure access controls to prevent unauthorised access to sensitive information.

Furthermore, it should be noted that closed source solutions introduce risks like dependency on a single vendor, do not facilitate the required levels of resilience against compromising, or do not provide evidence that all needed security measurements are implemented.

### Dependencies

*Focus area: Establish EU Ecosystem for Open Hardware: Hardware like servers, network or storage* equipment, as well as the appropriate infrastructure by means of teams, know-how, and research and development based in EU.

### Relevant use cases / application domains

This technology priority fulfils the requirements and provides the respective added value in several use cases, since appropriate operating systems are needed for any edge device. Moreover, the adoption and improvement of operating systems affects the *infrastructure – edge-to-cloud continuum* use case as appropriate operating systems are needed.

## *Recommendations*

| | |
|---|---|
| *Short-term* | Continue the support of an open source strategy following the "Think Open" theme of the EU, since it promotes the sharing and reuse of software solutions, knowledge, and expertise, to deliver better European services that benefit society and lower costs to that society, while also being strategic in several areas [155]. |
| *Short/mid-term* | Establish a European Competence Centre for Open Source. An EU-wide competence centre for open source (operating systems) would provide a central location for expertise and resources related to these systems. It would enable the sharing of knowledge and best practices across the EU, leading to more efficient and effective use of open source. The competence centre could also serve as a hub for research and development, promoting innovation and the development of new open source systems, by supporting, exploiting and extending – where possible – existing standards / projects / initiatives such as Anuket, CAMARA, LFEdge, etc. It could help to promote the adoption of open source within the EU, particularly among small and medium-sized enterprises. An EU-wide competence centre would also facilitate collaboration and partnerships between different organisations and stakeholders within the EU. It could help to standardise and harmonise the use of open source across the EU, reducing the risk of vendor lock-in and increasing flexibility. By promoting the use of open source, the competence centre could also contribute to the EU's digital sovereignty and independence. EU-supported action will establish the connections between different research institutes (universities) and define the organisational and technical background of a European Competence Centre for Open-Source. One goal is to support the EU Open Source software strategy and identify other funding sources like governments or corporate sponsorship. The centre will launch research and development programs to address key challenges in the volatile ecosystem of open source software. |
| *Mid/long-term* | Establish a long-term open source strategy in collaboration with an EU Competence Centre for Open-Source. |
| *Long-term* | The *European Competence Centre for Open-Source* will build a community and include researchers, developers, and other stakeholders to support goals and activities. Focus on education and training: the different institutions, companies, |

and public sectors must build knowledge to make optimal use of the Competence Centre.

## 8.6. Technology Priority: Improving Software for Hardware Operation, Management, and Monitoring

### Key drivers

Current solutions in software for hardware operation, management, and monitoring are focused on increasing efficiency, reliability, and security. Automation and machine learning technologies are being used to automate and optimise tasks such as provisioning, deployment, and maintenance. Monitoring and alerting systems are being developed to enable real-time monitoring of hardware performance and to identify potential issues before they become problems. Documentation and training are being emphasized to ensure that hardware operation and management processes are performed consistently and correctly. Integration with other systems, such as IT service management and incident management tools, is becoming more common to improve visibility and coordination of hardware-related tasks and issues. Security is a top concern, with a focus on encryption, access controls, and regular security assessments to prevent unauthorised access or tampering. The use of open source software and hardware is becoming more widespread as a way to increase flexibility and reduce vendor lock-in. Cloud computing is also playing a significant role, with the development of software tools and platforms to enable the management and monitoring of hardware in a cloud environment. Industry standards and best practices, such as the IT Infrastructure Library (ITIL), are being used to guide the development and improvement of software for hardware operation, management, and monitoring.

In this context, a cloud continuum introduces challenges when it comes to pure numbers: instead of hundreds or maybe thousands of devices (servers, switches, storage, etc.) there will be millions of devices. In addition, these devices will be a diversity of hardware and operating systems. Especially in edge scenarios, the communication on the control (management) plane will not be reliable and will have shortcomings, like limited bandwidth or high latency.

For new use cases there is the need to implement new features or improve the current situation. As an example, some parts of the cloud continuum might be switched off during low-load situations (e.g. at night or over the weekend). Such a functionality is currently missing in the management systems; the monitoring systems need to cope with this and not emit false alarms when equipment like a server or even a site is not reachable. There is also the need to improve existing functionality, as a ‘fast boot’ to be able to use a unit in seconds and not wait minutes for a unit to become ready.

### Dependencies

*Focus area: Standards for a Uniform Abstraction Layer:* Definition of the federation API.

### Relevant use cases / application domains

The improvement of management and operations software directly affects the *infrastructure – edge-to-cloud continuum* use case, since most of this type of software will be used across several infrastructures.

### *Recommendations*

| | |
|---|---|
| *Short/mid-term* | Management and monitoring systems must evolve in such a way that they are able to handle a huge number of heterogeneous devices. Management and monitoring systems need to be able to cope with failures and shortcomings - especially those of the network. To this end, a standardised control plane for hardware, management, and monitoring needs to be established. Additionally, management and monitoring need to be improved by implementing new features and enhancing existing ones, as they will be needed for a cloud continuum to operate, for example through AI-based prediction models. |
| *Mid-term* | The implementation of management and monitoring systems needs to be done by the hardware or software providers. Nevertheless, there is a need to standardise the management and control interface, which can handle the different services, use cases and (edge-) site requirements. |

# SECTION 9: INFRASTRUCTURE AND PLATFORM SERVICES

Infrastructure and platform services are the offerings available on the edge-to-cloud continuum to be ordered and consumed for the main purpose of building or scaling applications. Global public cloud provider services are the most frequent choice, due to their large and integrated offering. To increase competitiveness and build valid alternatives, the European market should strengthen its offer, grouping the currently fragmented stand-alone solutions into a federated offer, exploiting open standards and standardising them in terms of minimum scalability, openness, and transparency. Although some basic cloud services for compute, storage, and networking are now common, interoperability across the edge-to-cloud continuum is still to be achieved. This evolution of offerings at the edge is also driven by new, emerging technologies that significantly increase the quality and the quantity of computing, such as quantum computing, or the level of security in distributed architectures, such as blockchains.

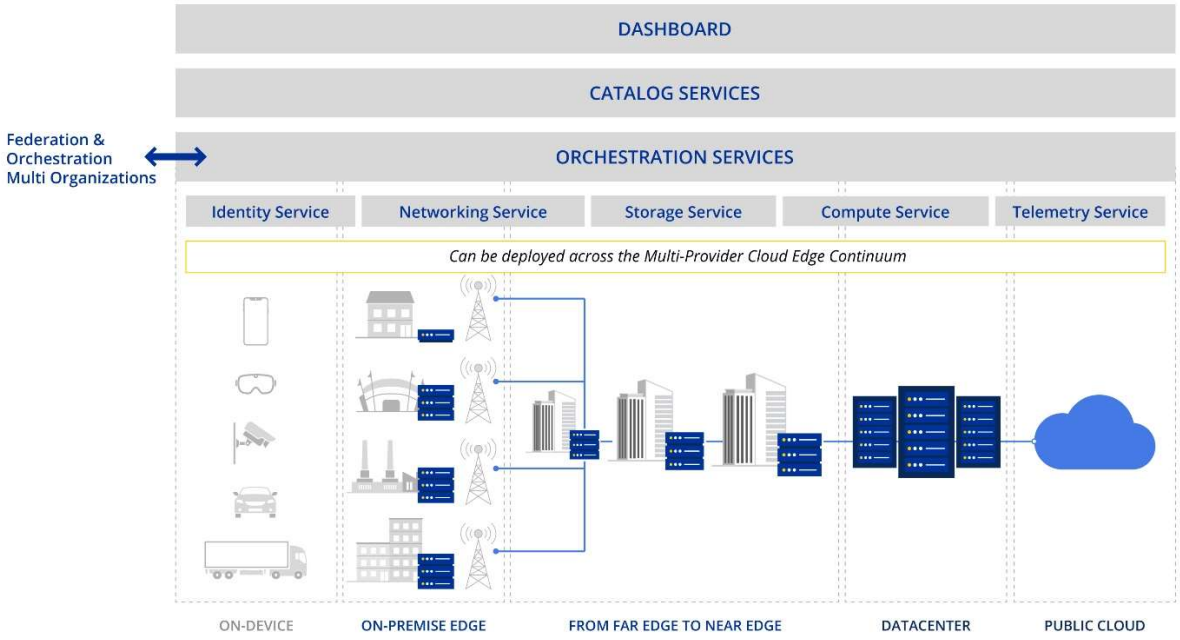



*Figure 28: Infrastructure and platform services*

To ensure consistency, some "generic" requirements must be considered for the respective services. Services should be developed and used in line with data regulations and policies. They should be made available through a service catalogue with standardised interfaces, while also advertising and reporting on their carbon footprint and offering carbon footprint optimisation options. Moreover, services should maximize the scalability, portability, and interoperability of workload across service providers and technology foundations. Finally, services should include storage support application mobility across the edge-to-cloud continuum as well as user mobility across locations.

# Focus area: Edge-to-Cloud Service Life Cycle Management

## 9.1. Technology Priority: Edge-to-Cloud Service Management Open Specification & APIs

### Key drivers

Most current cloud offerings are based on some open source cloud, storage, orchestration and networking solutions. These open source solutions are dynamic, continually developing software platforms. A quick look at the Cloud Native Computing Foundation landscape provide a glimpse of the ecosystem and all the functions required [157]. No single European firm can develop a unified, standardised and interoperable edge-to-cloud service management platform on its own, thus there is a need for open source software components that will meet the needs of European cloud players/providers (in terms of sovereignty, security and interoperability across regions). An ecosystem is required to build it, like the European Cloud Industrial Alliance (EUCLIDIA) [29]. One of the biggest issues to be developed and improved in the available open source platforms through open ecosystems is related to scalability and interoperability. Standardised components must consider these drivers in different areas: (i) computing area for clouds with hundreds and thousands of compute nodes, (ii) storage area for network storage systems with capacity of hundreds of petabytes, (iii) networking area to support hundreds / thousands of compute and storage nodes, (iv) interoperability area with multi-regional or multi-zone solutions for hundreds of edge nodes, and (v) security area to enable authentication, authorization, and accounting (AAA) with hundreds of federated entities.

### Relevant use cases / application domains

Open Specifications and APIs are a core enabler for most, but not to say all, services to be run on an edge-to-cloud continuum. As expressed those specifications and APIs are fundamental and therefore relevant for all the listed use cases. The *smart city* and the *AI federated machine learning* use cases are representative ones. Solutions for smart cities are characterized by a wide variety of providers, users, and industries. Therefore, the establishment of open specifications and APIs leads to a harmonisation of, for example, connectors in data-driven applications and therefore to a reduction of complexity and to the simplification of application development.

### *Recommendations*

| | |
|---|---|
| *Short-term* | Deliver a European cloud and edge platform open specification and APIs that reduce or remove dependency on “as a service” infrastructure products from non-EU players. The availability of such a platform stack specification and subsequent software offerings will enable European cloud and edge players to focus more on innovation by providing the base components needed to develop higher-level |

cloud services related to edge, AI, and big data. This platform stack will be built on standardised and open interfaces to find, request, and operate services. It will allow the expression of technology dependencies (on specific underlying technologies such as hardware acceleration), service dependencies (that may or may not be provided by the platform) and placement constraints (ensuring security and sustainability requirements are met while maximizing the benefits from the edge-to-cloud continuum). This platform stack is the very foundation of the subsequent services described in this section. As such, it is high priority and must be specified and result in subsequent development efforts within the next 3 years.

## 9.2. Technology Priority: Edge-to-Cloud Dynamic Application Lifecycle Orchestration Engine

### Key drivers

Given the continuous update of end users' applications [158] and devices, and the growing adoption of DevOps practices in Enterprises [159], the applications deployed on the edge-to-cloud continuum will demand similar mechanisms for deploying updates and upgrades. Deprecated or unused services should also readily be uninstalled from the infrastructure. Such solutions are available for centralised systems such as cloud infrastructures, but are not optimal to manage in a distributed computing landscape for the following reasons:

- Number of application instances: instead of a central application instance or application instances by region, there might be hundreds if not thousands of instances to manage.
- Heterogeneity of the landscape: the previously mentioned application instances would be deployed across an edge-to-cloud continuum with different capabilities, which might require different deployment configuration and mechanisms.
- User and machine mobility across locations and different types of access networks that require a much more dynamic orchestration. Indeed, due to the limited capacity of edge nodes, it is not possible to deploy all applications everywhere and have them running all the time. Instead of a deployment triggered by development teams, an event-based orchestration system revolving around the users is the best way to address this efficiently.

### Dependencies

*5.3. Technology Priority: Multi-provider Meta-Orchestration and Workload* Optimisation*:* Leading European providers with relevant open source software developers to work together in the creation and maintenance of a community-driven life cycle orchestration engine.

*5.4.* Technology Priority: Multi-provider Edge Cloud Federation*:* Fundamental to orchestrate the life cycle of applications across multiple services, providers, and regions / zones.

*6.2. Technology Priority: Advanced Simulation and Prediction Capabilities for* Operation*:* This will be essential to orchestrate the life cycle of applications across multiple suppliers and regions/zones.

### Relevant use cases / application domains

A dynamic application life cycle orchestration engine is fundamental to guarantee that the desired application is always used to provide services across the edge-to-cloud continuum. Therefore, such an engine is relevant for all listed use cases, while representative use cases and the added value of an orchestration engine follow.

In the *infrastructure – edge-to-cloud continuum* use case**,** applications will be operational in various regions and most likely on various service providers, and in a federated manner. To ensure consistency in the actual output, the application owner should be able to dynamically orchestrate application versions and release them along the application lifecycle and during runtime.

In the *digital twins* use case, digital twins may be used to emulate the behaviour of applications if the application owner enforces multiple releases of an application in order to secure a proper life cycle orchestration.

### *Recommendations*

| | |
|---|---|
| *Short-term* | Specify the short to mid-term requirements and desired performance goals. Build an initial solution architecture for the orchestration engine supporting: (i) environments dedicated to each application life cycle phase (e.g. development, testing, production), with the environments being pre-existing, pre-provisioned, or created on demand, (ii) the edge-to-cloud continuum, with application components deployed in a centralised but also distributed infrastructure; such distribution can be static (i.e. the topology is specified) or dynamic (i.e. based on policies and external events such as device mobility), and (iii) mobility across networks, taking into account data locality constraints. |
| *Mid-term* | Build a set of open source APIs for the orchestration engine to foster adoption across open source and commercial projects, so as to ensure the required integration with the broader orchestration mechanisms related to federation and also network standards integration. |

## 9.3. Technology Priority: End-to-End Quality of Service As Code

### Key drivers

Most existing edge computing use cases are mainly prototypes in private deployments with low complexity regarding infrastructure and networks making it easier to guarantee quality of service. The few mobile use cases already deployed at scale encounter lots of complexity because of the

heterogeneity already existing within the mobile network. Some solutions integrate applications into the radio network, such as MEC (Multi-Access Edge Computing), providing an edge abstraction layer and automation capabilities able to handle the workload in very close proximity to the user, fully leveraging network capabilities. MEC today is mostly integrated into the radio network.

When considering the complete edge-to-cloud continuum at scale, there are two key challenges to ensure end-to-end quality of service with respect to application developers' concerns: (i) planning the right infrastructure and network architecture blueprint required to guarantee the quality of service, which is a complex task due to the heterogeneity across the continuum, and (ii) deploying the applications on the right infrastructure and network resources based on their availability and considering potential user mobility geographically, across operators and across networks. The latter should also consider dynamic adjustment based on the infrastructure and network health.

Application developers cannot be expected to manage the aforementioned complexity in planning and operations. Platform solutions capable of managing the trade-off between the computational power and the narrow spaces of the edge, and able to handle a distributed workload and a heterogeneous deployment, are crucial to ensure the expected quality of service. Key to ensuring adoption by application developers and an outstanding user experience is the definition of how to express the quality of service requirements so that platforms can leverage the underlying infrastructure and network technologies, during deployment and operation of the business service.

### Dependencies

*7.1. Technology Priority: Device Connectivity for a True Edge* Experience*:* Delivers a stable and quality edge connectivity.

*7.2. Technology Priority: Control & Orchestration for Edge Connectivity at* Scale*:* Provides orchestration functions for dynamic connectivity control

*8.4. Technology Priority: Define and Implement the Infrastructure management & control* interface*:* Provides a standardised communication interface towards the actual physical connectivity layer.

### Relevant use cases / application domains

End-to-end quality of services is a relevant enabler for all use cases listed in the roadmap. Representative use cases are listed below:

The *smart & secure mobility* use case will benefit from easy-to-implement and reliable end-to-end quality of services as code in particular as those cases typically involve mobile entities and portability of applications.

With regards to technology use cases, the *infrastructure – edge-to-cloud continuum* use case benefits most from end-to-end quality of services as code due to its scalability and portability across the continuum.

***Recommendations***

| | |
|---|---|
| *Short-term* | Define models for the specification of services with the respective quality of service requirements. These should include the ability to specify bandwidth, latency, security, and technology requirements to deliver the expected user experience. The specification of each service should be done in a common format for all service providers. This should be the necessary first step to enable service offerings with the correct SLA and with a minimum level of monitoring. This would require a shared model regarding SLA and performance metrics so that requirements can be expressed, orchestrated, and operated more easily. Take into consideration that the recipes that abide by the service specification must be readable by the meta-orchestration and multi-federation mechanism described in Section 5. |
| *Mid-term* | Define and implement an open source abstraction API that hides the complexity from the application developer while allowing deployment and operation across the end-to-end edge-to-cloud continuum topology, across data centre, cloud, edge, and end -user networks, including their interconnection. Multi-Access Edge Computing platforms currently seem the solution best suited to provide such interfaces (e.g. unique API) in order to ensure that applications can be deployed on the infrastructure across the continuum and fully leverage available networks (Wi-Fi, 4G/5G, from different providers). |

# Focus area: Edge-to-Cloud Serverless Services

## 9.4. Technology Priority: Edge-to-Cloud Serverless Service

### Key drivers

The term "serverless computing" includes any operational model where all provisioning, scaling, monitoring, and configuration of the compute infrastructure are delegated to the platform. It is not a new concept but commercial offerings from hyperscalers such as AWS Lambda, Azure Container Instances, and Google Cloud Run contributed to its recent adoption in enterprises. Serverless computing allows developers to invest more time in developing code and less in managing the infrastructure. Indeed, servers are invisible to the user. It can be considered as an "abstraction" of the actual servers required to process a task (hence the original name of FaaS - Function as a service). Serverless technology includes not only cloud functions but also hosted containers to deploy code rapidly without needing to manage the underlying infrastructure. Taking advantage of serverless computing, development teams can very quickly build scalable applications, while agility and flexibility are guaranteed for future workloads.

As declared by Gartner on its "Emerging Technology Roadmap for Midsize Enterprises" [160], the focus is on serverless architectures: companies are adopting modern software development methodologies, especially in front-end operations technology, while modernising legacy back-end infrastructure. CIOs view serverless computing as a low-risk, high-value investment that allows to reduce the time to market and permits administrators to improve agility on infrastructure management.

Currently the most used serverless framework is Knative, open source from 2021, however the standardisation of serverless computing is still under development. Indeed, the previously mentioned successful offerings, especially FaaS, are provider specific, not only in terms of their API but also the ecosystem the serverless workload can leverage. A more open and interoperable approach would see more development teams and communities to create new tools and frameworks to meet specific business and security requirements. In a wide range of computing settings, from resource-constrained edge devices to highly virtualised cloud platforms, EDGELESS is designed to perform serverless computing effectively. It will enable autonomous deployment and reconfiguration to fully utilise the computational capabilities present in clusters of neighbouring edge nodes by utilising AI/ML technologies. EDGELESS will define novel orchestration systems that offer a flexible, scalable horizontal compute solution capable of fully utilising diverse edge resources, while keeping serverless' advantages, such as its application programming paradigm, and vertical integration with the cloud. This challenging task will be accomplished by using distributed computing techniques to divide the edge environment into clusters, each of which will be run as a local decentralised serverless platform. Dynamically concentrating resources, either physically or conceptually, at the expense of other resources will increase environmental sustainability.

Moreover, with the constant increase in data to be processed and devices to be managed, serverless computing services should expand beyond cloud offerings and be integrated into an edge-cloud platform providing open and interoperable AI, quantum computing, and blockchain services to achieve high application performance in term of runtime latency, dynamic workload distribution, computing speed, and security.

### Dependencies

*3.1. Technology Priority: Sustainability by* Design*:* Use only the resources needed for a specific function/service.

*5.3. Technology Priority: Multi-provider Meta-Orchestration and Workload* Optimisation*:* Leading European providers with relevant open source software developers to work together in the creation of a community-managed platform capable of solving the key federation challenges in the edge-to-cloud continuum.

*5.1. Technology Priority: Open Standards for Cloud Infrastructure* Services*:* Ensure EU is represented and influential in existing standardisation and normative bodies.

*6.2. Technology Priority: Advanced Simulation and Prediction Capabilities for* Operation*:* This will be essential to optimise and distribute workloads across regions / zones.

*8.6. Technology Priority: Improving Software for Hardware Operation, Management, and* Monitoring*:* This is fundamental to ensure redundancy, availability, and control.

*10.2. Technology Priority: Data Spaces and* Networks*:* Serverless infrastructure will lay the basis for data spaces and distributed network implementation.

### Relevant use cases / application domains

Regarding use cases, serverless is a relevant enabler for all use cases listed in the roadmap. Representative ones are listed below:

The *cross-industry decarbonisation data platforms* use case is strongly impacted by serverless technology, which enables an efficient use of resources at the time and place in which they are needed.

Regarding the technology use cases, the infrastructure use case related to the *edge-to-cloud continuum* is the one that is most affected by serverless architecture due to its scalability and portability across the continuum.

### *Recommendations*

| | |
|---|---|
| *Short-term* | Move to open source serverless platforms in order to make the landscape more balanced, addressing the fact that many services are now built in hyperscale environments with a high risk of lock in. Open source stacks will also facilitate the portability of services, allowing them to be deployed across the edge-to-cloud continuum wherever they are needed. |
| *Short-term* | Put in place guidelines and regulations for cost transparency in order to protect the consumers and customers. Deliver approaches / means for customers to control costs related to scalable services. |
| *Mid-term* | Focus on application modernisation, subsidizing the transformation of legacy applications into serverless ones from scratch, instead of introducing only quick-win adjustments. Foster a more structural approach in the transformation of the current application landscape to realise the full potential of serverless. |
| *Long-term* | Agree and share amongst developers and architects guidelines and best practices on when the serverless approach can yield the most benefits. This will increase the optimum use of the technology, i.e. when and where it is needed. |

## 9.5. Technology Priority: Edge-to-Cloud HPC Serverless Service

### Key drivers

Exploring the latest High Performance Computing (HPC) models can be crucial for use cases such as intensive data processing with deep learning algorithms. HPC models have been the same for decades: large computer clusters with monolithic middleware. Cloud merely provided a new option by renting a grid elsewhere, an opportunity to reduce cost but not enough to align with the agility and new technologies used by enterprises. Indeed, HPC services are lagging, not cloud native, nor linked to AI technologies. HPC services were also never designed to take advantage of fully distributed infrastructure. Some initiatives to explore HPC potential are underway, for example the HPC, quantum computing-based LEONARDO project in Bologna Technopole (aiming to cover 20% of the European computational needs) [161]. Serverless HPC over Cloud (Shoc), published in the Bulgarian Academy of Science [162], provides a reference architecture to execute HPC by leveraging serverless services. More investments and capillary endeavours are needed to make this technology available at scale to industries.

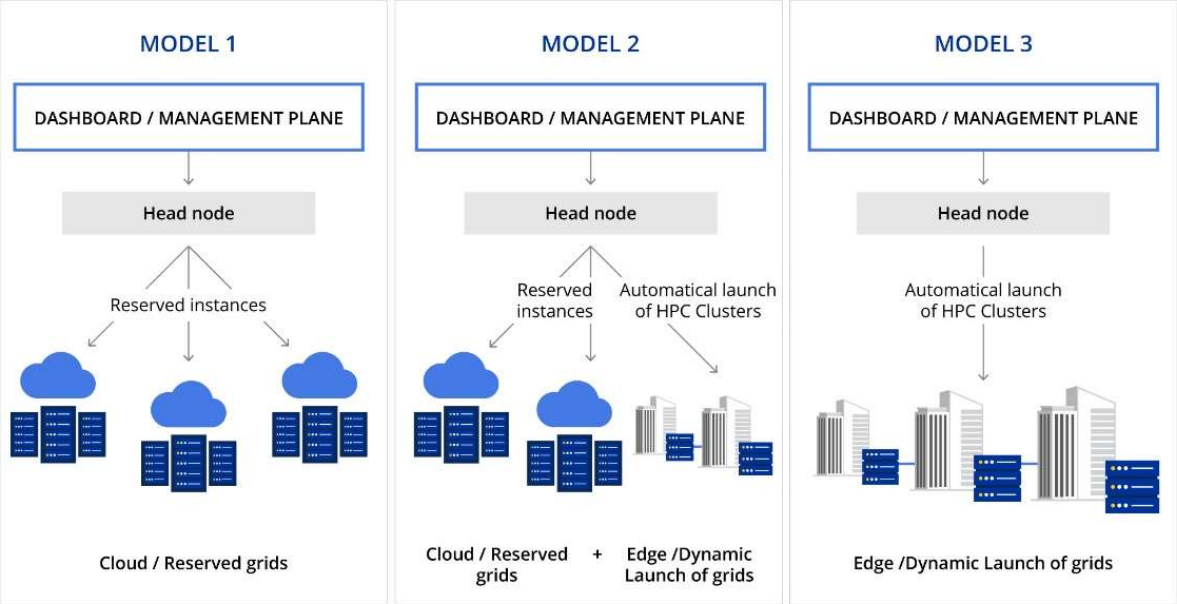



*Figure 29: Edge to Cloud HPC Serverless Services*

### Dependencies

*7.2. Technology Priority: Control & Orchestration for Edge Connectivity at* Scale*:* The development of standard and open Network-as-a-Service (NaaS) APIs will provide the means to implement these features more efficiently.

*5.3. Technology Priority: Multi-provider Meta-Orchestration and Workload* Optimisation*:* Leading European providers with relevant open source software developers to work together in the creation of a community-managed platform capable of solving the key federation challenges in the edge-to-cloud continuum.

*5.1. Technology Priority: Open Standards for Cloud Infrastructure* Services*:* Ensure EU is represented and influential in existing standardisation and normative bodies.

*5.2. Technology Priority: Uniform Abstraction Layer for Multi-provider* Portability*:* Follow open standards and open source software where possible to build the abstraction layer.

*8.1. Technology Priority: Establish an Open Hardware* Ecosystem*:* Define and standardise open hardware based on existing standards for different use cases through the cloud continuum.

*9.7. Technology Priority: Edge-to-Cloud Data* Services*:* Build a scalable open source data solution to manage data exchanges between massively distributed and heterogeneous actors over the edge-to-cloud continuum.

*10.1. Technology Priority: Data as a Competitive Advantage for* Europe*:* Build upon the existing EU regulations and open standards to promote data and applications.

### Relevant use cases / application domains

Urban growth requires a shift of the mobility / transport system towards optimised energy and resource consumption, and usability as described in the *smart and secure mobility* use case. Mobility as a service and autonomous driving solutions require real-time data exchange between devices and scalable capacity to run AI models in the cloud.

*Smart city* services optimise resource usage and improve the quality of life by connecting and utilising data from different sectors (e.g. power plant, utilities, infrastructure, health, mobility, etc.). As data processing is the enabler for smart cities, the digital infrastructure from edge to cloud is a key/critical success factor to providing the right data at the right time and to ensuring data/digital sovereignty.

In both of these use cases, serverless HPC services would allow the business demand to be met while ensuring energy and resource optimisation, leveraging both cloud and close proximity edge nodes.

### *Recommendations*

| | |
|---|---|
| *Short-term* | Provide HPC services without having to reserve a grid. Deliver new classes of hardware, software, and IP for hosting highly accelerated processing, machine learning or low-latency applications at the edge. Dynamically reorganise resources |

| | |
|---|---|
| | to enable the launch of HPC clusters when applications / situations are needed enable to optimise resources' uses. |
| *Mid-term* | Distribute HPC services across edge and cloud environments. Facilitate AI/ML services at the edge and across the continuum through the provision of HPC services at the edge (also accelerating use cases in key industries such as mobility and manufacturing). Introduce easy-to-use GPU acceleration services, as also highlighted in [163]. |

# Focus area: Edge-to-Cloud Innovative Platform Services

## 9.6. Technology Priority: Edge-to-Cloud Quantum Computing Services

### Key drivers

The possibility of developing a quantum computer sophisticated enough to execute Shor's algorithm for large numbers has been a primary motivator for advancing the field of quantum computation. In general, it is believed that quantum computers will help immensely with problems related to optimisation, which plays key roles in everything from defence to financial trading [164]. Currently, the use of Quantum Computing (QC), due to the high implementation costs, has the cloud as its main option, and most of the implemented use cases are not in production. However, in the mid to long run, QC is expected to be also used at the edge nodes for computing and to enable the capability to manage massive quantities of data for load balancing and dynamic resource provisioning scenarios [165].

The full potential of this technology is not yet realised and future research is open to reducing current limitations, such as "noisy" outputs (i.e. with high error rates) and the possibility to use quantum entanglement to secure transfer data. 43% of organisations working on quantum technologies expect them to become available for use in at least one major commercial application within the next 3–5 years [166].

In this context, several providers are putting efforts towards releasing the full potential of QC. In 2021 Google Cloud announced teaming up with quantum computing startup IonQ to make its quantum hardware accessible through its cloud computing platform. In 2022 Amazon Braket (AWS) added support for Borealis, a new photonic quantum processing unit (QPU) from the Canadian Xanadu, the first publicly accessible quantum computer that is claimed to offer quantum advantage. Joint efforts are also underway. In 2022, the Lombardy Region, the Municipality of Milan, the Polytechnic university of Milan, Aria, the Intesa Sanpaolo Bank, and the First Regiment of Transmissions of the Italian Army signed an MoU for the birth of the first worldwide, ultra-safe, quantum network, setting Milan as the candidate for the "Worldwide Capital of Quantum Computing".

### Dependencies

The dependencies identified below are not technical prerequisites but initiatives which need to progress to ensure any kind of scale is possible.

*Focus area: Advanced applications:* Foster the development of an open marketplace for data and cloud that will leverage scalability and network effects by providing an open European application marketplace to facilitate dissemination and exploitation.

*10.1. Technology Priority: Data as a Competitive Advantage for* Europe*:* To build upon the existing EU regulations and open standards to promote data and applications.

*5.2. Technology Priority: Uniform Abstraction Layer for Multi-provider* Portability*:* Follow open standards and open source software where possible to build the abstraction layer.

*5.3. Technology Priority: Multi-provider Meta-Orchestration and Workload* Optimisation*:* Leading European providers with relevant open source software developers to work together in the creation of a community-managed platform capable of solving the key federation challenges in the edge-to-cloud continuum.

### Relevant use cases / application domains

One of the main concepts in the computing continuum is the use of caching to bring the intelligence closer to the edge instead of leaving the intelligence centralised in cloud servers. AI federated machine learning at the edge trains AI models across edge nodes without the need to transfer data to the cloud to preserve privacy and bandwidth. Quantum computing at the edge could allow faster training of the AI models, pushing the boundaries of what is possible with AI at the edge.

A prerequisite for the linking Operational Technologies (OT) systems to IT representation use cases is the capability to make data from physical devices (e.g. factories, machines, cars, medical operation rooms) available to an IT system which is able to process and analyse the data and drive actions back to the physical world (closed loop). Quantum computing, especially at the edge, could allow new breakthroughs in terms of near real-time simulation of complex systems.

### *Recommendations*

| | |
|---|---|
| *Short-term* | Foster the quantum twin concept, which is not a contradiction in terms but instead describes a hybrid approach that can be implemented using the technologies available today by combining classical computing and digital twin concepts with quantum processing. |
| *Mid-term* | Build quantum communication, quantum computing, quantum simulation, quantum metrology and sensing services, and integrate them in European cloud infrastructures. |

| | |
|---|---|
| *Long-term* | Build quantum communication, quantum computing, quantum simulation, quantum metrology and sensing services across the edge-to-cloud continuum. |

## 9.7. Technology Priority: Edge-to-Cloud Data Services

### Key drivers

Today, there is no technical solution available to manage data exchanges over massively distributed and heterogeneous actors compliant with the Data Act. This EU regulation introduces the notion of data spaces, which is a set of standards and governance mechanisms aiming at fostering data exchanges between collaborative parties.

Additionally, there is an ever-increasing number of IIoT and edge devices which are producing large amounts of data that needs to be consumed from multiple actors spread across the cloud continuum. A solution is needed to support the sectoral data spaces that are emerging thanks to European initiatives, IIoT/edge devices, and the digital policy that the EU is implementing.

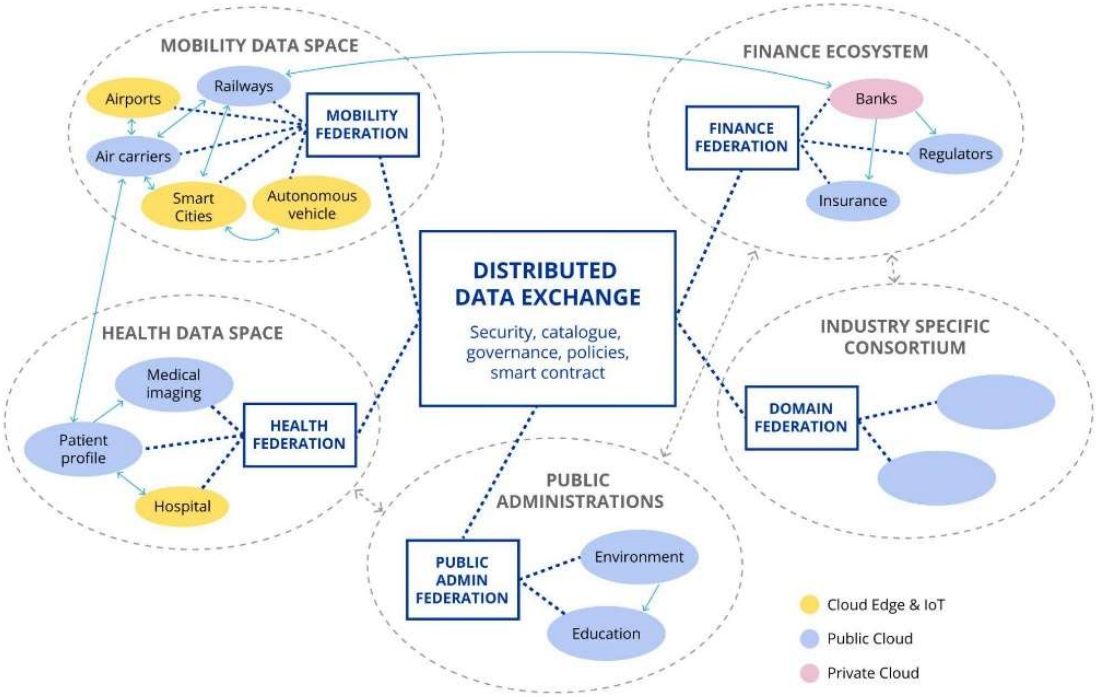



*Figure 30: Distributed data exchange*

The Horizon programme of the European Commission is proposing calls on the way to optimise Data Processing within the edge-to-cloud continuum, mainly for Innovation Actions and any other data consumers (HORIZON-CL4-2023-DATA-01-04 and HORIZON-CL4-2022-DATA-01-02). With TRL5 by the end of the projects, the expected outcomes are focusing on process and method

description, but not industrialisation. These solutions should complement the data exchange solution that is needed.

There are several data platforms in the industry leveraging different technologies (some specific vendors, some from hyperscalers, some in-house solutions) but they do not offer the level of interoperability and the level of trust that are required to build data spaces that will be composed of various actors with different systems and cloud providers.

### Dependencies

The dependencies identified below are not technical prerequisites but initiatives which need to progress to ensure any kind of adoption at scale is possible.

*1.4. Deployment Priority: Data-Sharing Business* Models*:* The emergence of these business models will refine the requirements for the data platform.

*2.7. Technology Priority: Promote & Implement Local Processing* of Data*:* Local processing guidelines will again drive the distributed architecture of the data platform.

*4.1. Technology Priority: EU innovative Data Encryption Technologies including Quantum-safe & Privacy-enhancing* Encryptions: Security is key to the data platform, especially as this new generation of platform will be ultra-connected and distributed. This must not compromise the security of the data, therefore encryption innovation is key to the viability of this data platform.

### Relevant use cases / application domains

All use cases would benefit from the proposed recommendations given the data spaces' added-value, since for example they will enable new opportunities of cross-organisation collaboration, even across industries.

Industries relying on highly distributed value chain will be the most impacted, through use cases such as the *digital supply chain*, but even use cases in healthcare or emergency will benefit from the ability to exchange information at scale across organisations. It will allow new business models and services for enterprises and end users.

## *Recommendations*

| | |
|---|---|
| *Short-term* | Provide a scalable solution to manage data exchanges between massively distributed and heterogeneous actors over the edge-to-cloud continuum. This solution should be a federated application running on top of existing data platforms to: (i) manage distributed data exchange across companies of any size as well as IoT and edge devices, (ii) offer simple and standardised mechanisms to |

connect once and exchange with many, without having to change technologies, (iii) give full data access and usage control to data producers, (iv) support the next-generation of data-driven applications, (v) focus on data exchange security (zero-trust) and data privacy by design, and (vi) be sustainable by design, reducing data transit and storage to the strict minimum.

This solution must be open source to ensure large adoption (see relevant recommendations in Section 1) and should embrace the data mesh paradigm that ensures no data centralisation, redistribution, duplication, and inconsistency, as is the case with data lakes (data needs to be consumed from the source of truth, i.e. directly from the data producers' information system). Data owners will remain in control of their data by deciding what data is shared with each consumer, for how long, at what price, and whether it will be anonymised or not.

## 9.8. Technology Priority: Edge-to-Cloud Blockchain Services

### Key drivers

Blockchain technology is very effective for providing trust in a distributed system. Synergies with quantum computing, which provides large-scale computation, could compensate for the highly demanding processing of some implementations. Currently, blockchain and related decentralised services exist around many fragmented initiatives. At the European Scale, EBSI is a market-friendly distributed blockchain network based on open standards and a transparent governance model. The need is to create cross-border services for public administrations and their ecosystems.

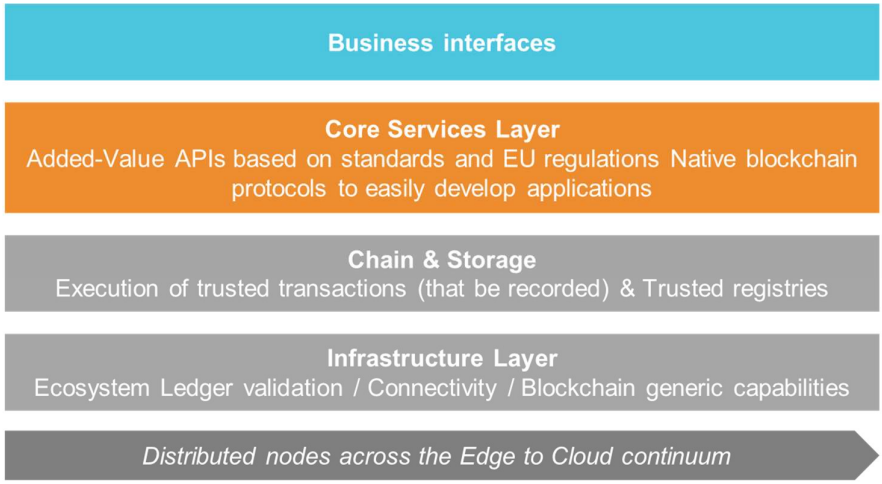



*Figure 31: EBSI model*

Blockchain technologies are supported by Europe through several innovation programmes, such as the Blockchain Strategy [167] and Ontochain [168], in order to accelerate their adoption through administrations and industries. It aims at supporting easy-to-use services to leverage blockchain capabilities. However, neither widely shared nor common European standards have been defined to cater for the mass implementation of blockchain.

### Dependencies

*8.3. Technology Priority: Implement Security from Ground up, Inherent in Every Aspect of the* Infrastructure*:* Ensure security of the infrastructure on which blockchain is deployed.

*8.6. Technology Priority: Improving Software for Hardware Operation, Management, and* Monitoring*:* Ensure performance of distributed ledgers at scale.

### Relevant use cases / application domains

In the *next-gen engagement and human centricity* use case, the use of blockchain technology will allow trust to be built across the different organisations involved in healthcare, especially regarding patient data and journey.

In the *cross-industry decarbonisation data platforms* use case, ledgers can be used to exchange trusted information about the carbon footprint of materials and products. It can also enable circular economy.

Moreover, there are several potential use cases of blockchain based on its relevant characteristics under investigation, tracking and registry of data enabling traceability services like supply chain management, identity and authentication management, digital property and smart contracts, confidentiality or "zero trust" services are some good examples in the industry.

### *Recommendations*

| | |
|---|---|
| *Short-term* | Structure an open ecosystem to ensure decentralised collaborations and test different blockchains in order to find best alternatives for the different sectors and applications. Support the implementation of a set of normative guidelines and frameworks of standardised procedures for the implementation and operation of blockchains across the European continuum. Foster standardisation, easy-to-use tools, and interfaces within a strong European network, enabling developers to initiate valuable use cases within an open European ecosystem. |
| *Mid-term* | Develop a European blockchain service following the model of EBSI, through a "core services layer" with specific services needed to accelerate key use cases across European industries and above. This layer will provide: (i) capabilities to instantiate blockchain nodes efficiently, (ii) standardised APIs to facilitate application developments and ensure compliance (through common guidelines shared by users) with blockchain adoption and services' interoperability, (iii) a |

ledger (a log keeping a definitive record of transactions) and a distributed ledgers network (a distributed ledger is a ledger that has its entries stored across a series of nodes in a network, rather than in a single location making it "tamper-resistant") [169], and (iv) smart contracts related to events.

# SECTION 10: APPLICATION AND DATA SERVICES

To enable mass uptake of cloud and edge technologies by European stakeholders, it is necessary to make them easily accessible and applicable to multiple domains. The speed and efficiency of creating value-driven applications and sharing the data and information will determine the competitiveness of the European cloud and edge industry. Leveraging cloud and edge technologies in certain high-growth industries such as automotive, manufacturing, earth observation, or engineering will allow for subsequent introduction where it is less prolific. Among the industrial domains, manufacturing is a leading sector for the European industry, consequently manufacturing data represent a competitive advantage for Europe. Collaboration across the product development life cycle is critical for these enterprises and they also have to span increasingly complex business environments that bring together multiple companies, each with their own systems and processes. This challenge of global communication of product data can only be solved by a common understanding of the shared data; it also requires an agreed data model for industrial data to be publicly available.

The development of digital commons is rooted in the democratization of the FLOSS (Free Libre and Open Source Software) movement's methodology and values. This is based on a decentralised, peer production of data sharing architectures and the reference source code, allowing open collaboration as well as possible modification and redistribution. Beyond FLOSS, digital commons enable the development of open data and open standards to the benefit of knowledge sharing, democratic progress, and economic growth. By pooling large communities and relying on open licence, digital commons are tremendous generators and sharers of data (Digital Commons Report European Commission). As part of the French Presidency of the Council of the European Union, a call for the creation of a European working team focused on proposing a European Initiative for Digital Commons was issued in the "Declaration by the Presidency of the Council of the European Union calling for a European Initiative for Digital Commons".

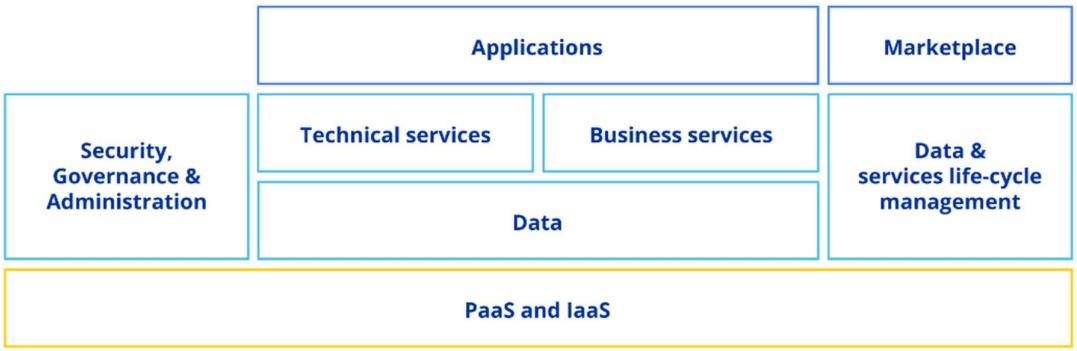



*Figure 32: Application and data services*

To push data economy and the application of data services, the governance structures around trusted data value creation are necessary, relying on data regulation and standards as well as norms based on European values.

In this context, this section discusses the two main requirements regarding: (i) the need for large-scale data sharing platforms applicable to any business/industry, and (ii) the commoditisation of the technical and business services necessary to bridge data and application layers.

# Focus area: Data Spaces

Data is described as the raw material of the 21st century economy. Access to this data is therefore an enormous strategic power. On one hand, big tech companies have control over a gigantic data quantity, on the other hand, a multitude of public and private actors control minor volumes of data, not always exploitable. It is, therefore, important that Europe supports federated data sharing by encouraging the creation of infrastructures that exploit, control, and share data, while also respecting European values and interests. The regulations (e.g. GDPR, DA, DGA, etc.) are set forward for this purpose and various initiatives have been launched to deploy and create data spaces.

Many organisations are working on the data space standardisation such as Gaia-X, IDSA [170], MyData [171], aNewGovernance [172], BDVA [22], and Fiware [173]. Projects like Catena-X, Smart Connected Supplier Network (SCSN), and Eona-X develop and operate standards for certain data spaces. In the case of Catena-X, for example, the automotive data space is being built to foster data sharing along the automotive supply chain. It is also worth noting that many use cases planned or under development have been described in detail and are published in the Gaia-X [174] position papers.

Furthermore, the European Commission is investing in the implementation of an open source smart middleware, Simpl [175], that will enable cloud-to-edge federations and support all major data initiatives funded by the European Commission, such as common European data spaces.

## 10.1. Technology Priority: Data as a Competitive Advantage for Europe

### Key drivers

To provide fair access to data for the benefit of European businesses, the EU needs to promote and regulate the data landscape. The *European Strategy for Data* aims at creating a European Single Market for data that will ensure Europe's global competitiveness and data sovereignty. Common European data spaces will ensure that more data becomes available for use in the economy and society, while keeping the companies and individuals who generate the data in control. In 2022, the Commission proposed a regulation on harmonised rules on fair access to and use of data (Data Act). The Data Act is one pillar of the European strategy for data (still under discussion and

processing at the moment). Its main objective is to make Europe a leader in the data economy by harnessing the potential of the ever-increasing amount of industrial data, to benefit the European economy and society.

Furthermore, in line with the FAIR principles (Findable, Accessible, Interoperable, and Reusable) [176], the overall objective is to make Europe the most successful area in the world in terms of data sharing and data re-use while respecting the legal framework relating to security and privacy in addition to fostering collaboration and building on existing initiatives.

### Dependencies

Even though data regulation is a prerequisite of many technical priorities, the following priorities address data regulation as part of their main recommendation and thus interdependencies are identified as follows:

*1.4. Deployment Priority: Data-Sharing Business* Models*:* Multi-sided business and market activities based on clear rules (e.g. for data sharing) to provide a secure legal framework for cross-vendor data sharing.

*2.3. Technology Priority: Operationalize Europe's Championing of Human-Centric & Other People-Centric* Values*:* Provide mechanisms to manage compliance and trust.2.5. Technology Priority: Make EU Regulations fit for a Digital Sovereign Europe*:* Align with global regulatory bodies to ensure an open market and interoperability.5.6. Deployment Priority: Federated Cloud Marketplace*:* Marketplaces will provide catalogues for cloud-edge data, applications, and infrastructure services which adhere to European regulation.

### Relevant use cases / application domains

There are several use cases that are relevant and promote data regulation. Representative ones include: (i) the *next-gen engagement and human centricity* use case, since the healthcare domain is very sensitive to data regulations, (ii) the *cross-industry decarbonisation data platforms* use case, considering the requirements of global warming requires regulations adopted by all, and (iii) the infrastructure on *mobile networks driving cloud edge*, given that telecommunications is a domain where data regulations are required to address interoperability requirements.

## *Recommendations*

| | |
|---|---|
| *Short-term* | Promote *Data as Digital Commons* to provide the community with free and easy access to information. Data created within digital commons will either remain in the digital commons or be reused for external purposes through various forms of open licensing. These data will empower new usages and enable business models to flourish. Digital commons will provide new possibilities for European businesses, market, research, and society, especially in relation to data economy and data science in areas such as computational infrastructure, software, AI |

models and data utilisation. Digital commons will increase interoperability and cost effectiveness while providing inclusive access to market and information, and enhanced possibilities for small and medium-sized enterprises and citizens.

## 10.2. Technology Priority: Data Spaces and Networks

### Key drivers

Common European data spaces and networks will ensure that more data becomes available for use in the economy and society while keeping companies and individuals in control of their data. The latter is also highlighted in the European Strategy for Data that focuses on a European Single Market for data.

Since data plays a major role in driving the European economy, *data life cycle management* ensures that the data available to users is accurate and reliable. Such an approach provides tools to manage data along their life cycle (from development to decommission/deletion), including log management, version management, status monitoring, certification and attestation.

Moreover, *data interoperability* is of importance since the availability of interoperable datasets within and across sectors and domains is one of the key success factors to drive the European data economy and industrial transformation. The data usually need to be integrated with other data. In addition, the data need to interoperate with applications or workflows for analysis, storage, and processing. According to FAIR principles: (i) (meta)data use a formal, accessible, shared, and broadly applicable language for knowledge representation, (ii) (meta)data use vocabularies that follow FAIR principles, and (iii) (meta)data include qualified references to other (meta)data.

### Dependencies

Data openness and interoperability are promoted by the following priorities, which are interdependent with the Data Spaces and Networks priority:

*1.4. Deployment Priority: Data-Sharing Business* Models*:* To provide organisational awareness and adoption of data platforms including new commercial mechanisms for data sharing2.5. Technology Priority: Make EU Regulations fit for a Digital Sovereign Europe*:* Align with global regulatory bodies to ensure an open market and interoperability.2.6. Technology Priority: Support Distributed & Interoperable Architectures*:* In line with the Digital Decade target for 2030 and European initiatives to foster digital sovereignty, decentralised architectures with distributed data processing and storage should be promoted starting in the short term and further expanding the capillarity of edge infrastructure.

*5.1. Technology Priority: Open Standards for Cloud Infrastructure* Services*:* Ensure EU is represented and influential in existing standardisation and normative bodies, align landscape of existing de-

facto bodies and associations and define standardisation landscape, provide open source reference implementations.

*5.2. Technology Priority: Uniform Abstraction Layer for Multi-provider* Portability*:* The abstraction layer allows the development of AI-enabled automation, discovery and identity services, and distributed core infrastructure components following open standards and open source software where possible.

*Focus area: Edge-to-Cloud Service Life Cycle Management:* Specify a cloud & edge software stack with standardised and open interfaces, and finally ensure their implementation in software offerings.

### Relevant use cases / application domains

Several use cases mandate data interoperability and openness. As examples, the *smart and secure mobility* use case and the *smart cities* use case are two use cases involving multiple stakeholders and consequently require interoperability at both data and application levels.

### *Recommendations*

| | |
|---|---|
| *Short-term* | Manage data as digital commons by promoting openness and data model standardisation in order to foster the development of data spaces and networks under the principles of interoperability and fair access to data. Enforce regulatory means and tools such as tender requirements or funding preferences to boost technological sovereignty and promote European ownership of the entire data life cycle. |

## Focus area: Advanced applications

The European Commission proposed two legislative initiatives to upgrade rules governing digital services in the EU, the Digital Services Act (DSA) and the Digital Markets Act (DMA). The Commission made the proposals in 2020 and in 2022 a political agreement was reached on both acts. The DSA and DMA have two main goals: (i) to create a safer digital space in which the fundamental rights of all users of digital services are protected, and (ii) to establish a level playing field to foster innovation, growth, and competitiveness, both in the European Single Market and globally. In order for businesses to be able to efficiently build sustainable added-value services on top of the data layer, the underlying technologies that intermediate between the data and application levels should be as transparent and standardised as possible. Their sovereignty should be ensured.

Additionally, edge computing offers many advantages regarding privacy. Processing personal information in a distributed fashion, near the user, tempers some of the privacy risks that have

arisen from the ravenous accumulation of data by corporations – particularly the Big Tech companies – in the past 20 years. However, crunching that data on smaller devices, potentially outside the corporate network, could also expose it to interception or loss. Nevertheless, edge computing may prove to be a net-positive for privacy if it catalyses technologies, such as federated learning and homomorphic encryption, that allow organisations to glean insight on their customers without hoarding personal data. Examples of such applications include AI applications manipulating voice or natural language as well as collaboration platforms such as digital workplaces or VR/AR Metaverse.

Simultaneously, the European industry is pursuing significant technological advancements over cloud-edge value chain under the IPCEI-CIS integrated project. The goal of the IPCEI-CIS project is thus to develop and initially roll-out the key interdependent building blocks and the associated horizontal requirements (such as sustainability, cybersecurity) along the strategic steps of the value chain of the Distributed Multi Provider Edge-to-Cloud Continuum. Such a continuum will be based upon a common end-to-end data processing infrastructure, enabling value creation via the provision of platform and application services across the EU, fulfilling key requirements of ultra-low latency, dynamic bandwidth, and cybersecurity. The project will interconnect cloud-edge computing by establishing the multi-provider edge-to-cloud continuum as technological basis for the initial roll-out of advanced data processing capabilities for key sectors such as automotive, manufacturing, energy, logistics, transport/mobility, tourism, education, or public services. The multi-provider edge-to-cloud continuum will deploy key digital technologies and applications like smart networks and services (e.g. AI, analytics), data driven robotics, common generic data space applications, and cloud-edge foundation services. The IPCEI-CIS will accelerate the cloud-edge uptake among SMEs, industries, and public administrations by addressing emerging data processing demand and will foster the EU global technological leadership in the cloud-edge sector. It has the potential to introduce first large-scale European cloud and edge systems, providing a required market push for wide adoption by application developers and their users.

## 10.3. Technology Priority: Enhanced Applications Development

### Key drivers

The efficiency of application development is a crucial success enabler since it will enable the rapid establishment of a large and active user ecosystem. Special features should be provided to facilitate application development. Such features also include aspects related to low code/no code application developments. This is a major market trend: Gartner estimate that the low-code market grew by 23% in 2020 to reach $11.3 billion and to $13.8 billion in 2021, and will be worth almost $30 billion by 2025. Gartner also forecasts that low-code application development will account for 65% of all application development activity by 2024, mostly for small and medium-sized projects.

In order for European businesses to be able to build sustainable added-value applications on top of the data layer, the underlying technologies that typically rely on the “platform” pattern, located

between the data and application levels, should be as transparent, standardised, and commoditised as possible. A platform is a business model that creates value by facilitating exchanges between two or more interdependent groups, usually consumers and producers. To make these exchanges happen, platforms harness and create large, scalable networks of users and resources that can be accessed on demand. Platforms create communities and markets with network effects that allow users to interact and transact. In this context marketplaces are emerging. A cloud marketplace is an online environment where customers can buy and manage cloud-based applications and licensing. According to Gartner, enterprise customers of all sizes buy over half of their services from cloud marketplaces, making them a cornerstone of a successful go-to-market strategy for providers looking to sell SaaS.

### Dependencies

Facilitating the development of applications is a need also addressed by the following recommendations, which are interdependent with the technology priority related to Enhanced Applications Development:5.6. Deployment Priority: Federated Cloud Marketplace*:* Marketplaces will provide catalogues for cloud-edge data, applications, and infrastructure services which adhere to European regulation.

*Focus area: Innovative Design, Operation:* Standardisation will foster optimisation of cost, performance, and energy consumption across all sites at any given point in time. Development of standardised designs for adequate resource discovery, allocation, management capabilities, and workload orchestration technologies.

*7.2. Technology Priority: Control & Orchestration for Edge Connectivity at* Scale*:* The development of standard and open Network-as-a-Service (NaaS) APIs, supported by new cloud-native, software-based technologies and by the 5G Core, will provide the means to implement these features more efficiently.

*Focus area: Edge-to-Cloud Service Life Cycle Management:* Build a service to orchestrate the application life cycle across the edge-to-cloud continuum within a service provider landscape and federated platforms.

### Relevant use cases / application domains

All use cases highlight the need for enhanced application development. As representative examples, the *next-gen engagement and human centricity* use case and the *smart cities* use case are contexts which, favouring the development of B2C applications, are more active as their design is facilitated.

### *Recommendations*

| | |
|---|---|
| *Short-term* | Establish an *open marketplace* where cloud application providers can offer new services complying with the interoperability requirements, to move towards an ecosystem for application discovery and sharing. Enhance the marketplace with a set of open and standardised APIs promoting interoperability and reversibility across vendors. |
| *Short-term* | Foster the *low code/no code* approach to facilitate applications' development by everyone with an emphasis on small and medium-sized projects that are expected to account for more than half of application developments in the coming years. |
| *Short-term* | Facilitate and promote methods and tools to migrate classical applications to the edge-to-cloud continuum. Migration strategies provide challenges that could be tackled through blueprints and dedicated tools. |
| *Mid-term* | Promote enterprise interoperability to facilitate agile collaboration all along the B2B supply chains. Enterprise interoperability tackles all aspects at the business level and the corresponding ones on the technical level as for example data and application interoperability or reduction of lock-in effects. |

## 10.4. Technology Priority: IIOT/AI Applications

#### Key drivers

Supporting the Industrial IoT (IIoT) domain will be an opportunity for European businesses since manufacturing, retail, and health are the leading sectors for sensors and connected objects. The IIoT domain produces large amounts of data that may benefit AI applications, which are very data-intensive. IIoT introduces many new challenges that cannot be adequately addressed by today's cloud and host computing models alone. Representative challenges include the stringent latency requirements, the fully controlled and tracked software deployment and update requirements, the network bandwidth constraints, the resource-constrained devices, the need for uninterrupted services with intermittent connectivity, as well as new security and privacy challenges. Filling the technology gaps in supporting IIoT will require a new architecture that distributes computing, control, storage, and networking functions closer to end-user devices. In edge computing, the massive data generated by different types of IIoT devices can be processed at the network edge instead of transmitting them to the centralised cloud infrastructure owing to bandwidth and energy consumption concerns. These developments are supported by the increased industrial semantic interoperability technologies and standards being developed globally like the Asset Administration Shell (AAS).

Furthermore, modern deep learning techniques have quickly become a key component in various AI applications. The high volume of AI data traffic and highly computational demands involved in typical deep learning applications, e.g. face recognition and human tracking in camera networks,

put significant pressure on the infrastructure of state-of-the-art cloud computing paradigm. There is a clear need to investigate suitable network architecture and control mechanisms to handle the processing of massive data in a secure and private manner. One way to address this issue is to train machine learning models by distributing the optimisation of model parameters over multiple machines. Federated Learning (and related decentralised approaches) have been proposed as an alternative setting: a shared global model is trained under the coordination of a central server, from a federation of participating devices. The participating devices are typically large in number and have slow or unstable internet connections.

### Dependencies

Most of the technical priorities and recommendation related to the platform layer are relevant to IIoT and ML in a distributed setting. Thus, interdependencies are identified as follows:

*Focus area: Edge-to-Cloud Service Life Cycle Management:* Specify a cloud & edge software stack with standardised and open interfaces, and finally ensure their implementation in software offerings. Build a service to orchestrate the application life cycle across the edge-to-cloud continuum within a service provider landscape and federated platforms.

*Focus area: Edge-to-Cloud* Serverless Services*:* Build solutions to provide HPC services distributed across the edge-to-cloud continuum.

*9.7. Technology Priority: Edge-to-Cloud Data* Services*:* Build a scalable open source data solution to manage data exchanges between massively distributed and heterogeneous actors over the edge-to-cloud continuum. This should be a federated application running on top of existing data platforms, implementing the service mesh paradigm.9.8. Technology Priority: Edge-to-Cloud Blockchain Services*:* Develop a European blockchain service following the model of EBSI.

### Relevant use cases / application domains

Many use cases involve artificial intelligence applications that take advantage of data from sensors (and therefore fall into the IIOT category). The most relevant ones are the *smart and secure mobility*, the *global freight and people logistics*, and the *smart cities* use cases. Obviously, the *AI federated machine learning* use case is dedicated to this domain.

### *Recommendations*

| | |
|---|---|
| *Short-term* | Promote *standard protocols and guidelines for IIoT implementation and management*. Since any form of the IIoT fundamentally depends on connectivity, joining together disparate devices and sensors to capture and harness useful information, it is crucial for standards to be agreed between the different stakeholders involved in order to achieve interoperability. Utilise these standard protocols to foster the development of distributed and AI/ML solutions, |

| | |
|---|---|
| | bypassing the need to move vast amounts of data and providing the ability to analyse data at the source. |
| *Short-term* | Promote research on the *federated ML* challenges to develop industrial solutions that go beyond the most basic use cases, such as with leaks of sensitive information since, even if the local data are not directly exposed, model parameters are exchanged. Deliver approaches enabling the measurement of how much each dataset contributes to the performance of a collective federated learning model, since from a business perspective this raises questions about how to share the future revenues derived from a federated learning-based ASR model, while from an engineering perspective it shows how to detect possible corrupted datasets or partners not playing by the rules. |
| *Mid-term* | Design algorithms maintaining *application QoS across the edge-to-cloud continuum*. SLA contracts should be defined at the federation level and enforced all along the cloud technology stack where conventional cloud SLAs are not suitable due to lack of the flexibility required for automatic enforcement in such a dynamic and heterogeneous environment. |

# SECTION 11: CHALLENGES OF THE COMPUTING CONTINUUM IN THE EUROPEAN MARKET

## 11.1. Cross-Territorial Consistency and Regulatory Landscape

*Key Driver:* Deployment of services in a geographically distributed edge-cloud system can be limited by specific national norms and laws. Localized rules or regulations could slow down deployment and adoption of the computing continuum.

*Main Recommendation:* Collaboration across European actors, including Member States, technology players, industries, and policy-makers to ensure consistency and alignment with European priorities. Proliferation of common norms and standards across Member States and the whole EU market.

## 11.2. Interoperability

*Key Driver:* Interoperability is a must to foster innovation and collaboration to build the edge-to-cloud continuum, especially for edge applications deployed across a wide geographic scale.

*Main Recommendation:* An industry pre-requisite, or a public regulation, shared across Europe specifying the definition and requirements of sovereignty.

## 11.3. Scaling-up within a Regulated and Competitive Environment

*Key Driver:* Regulation and competition laws might slow down the scale-up of solutions across Europe.

*Main Recommendation:* Establish clear guidance to allow scalability across Europe.

## 11.4. Supply Chain Disruptions

*Key Driver:* The current supply chain crisis could slow down technology development and deployment.

*Main Recommendation:* Ensure local options exist for components critical to technology development and deployment.

## 11.5. Shortage in Professional Competencies

*Key Driver:* A shortage of competencies and skills is an obstacle to accelerating the technologies' adoption across Europe, as well as high innovation costs to deploy technologies at scale.

*Main Recommendation:* Address not only the technology priorities but also their human and economic requirements, defining European talent retention policies.

## 11.6. Resource Heterogeneity

*Key Driver:* Resources heterogeneity across territories (e.g., different energy sources, etc.) could trigger concerns for the deployments of the technologies, leading to concerns about data processing becoming unavailable in some locations.

*Main Recommendation:* Transparent and unbiased algorithm and data-based decisions need to be considered within regulations. Deployment of technologies should be distributed across Europe.

## 11.7. Market Fragmentation

*Key Driver:* Deployment of a cloud continuum from the core to the edge requires substantial investments at infrastructure level. A very consolidated cloud market, such as in the US, can facilitate a cloud player's return of investment and let them invest further. On the contrary, the European cloud market is fragmented, often regional.

*Main Recommendation:* Avoid "excessive regulation" that may create the preconditions for market fragmentation and define a regulatory regime that provides complete harmonisation.

## 11.8. Sovereignty on Hardware and Software

*Key Driver:* There is a competency gap to compete with hyperscalers, mostly regarding silicon and software technologies, which today are almost completely dominated by non-EU companies.

*Main Recommendation:* Find new tools and collaboration mechanisms towards the EU goal of achieving software and hardware sovereignty in the cloud-edge landscape, leveraging, promoting and protecting the open source innovation model as much as possible.

## 11.9. Security and Safety

*Key Driver:* Advanced services in cloud-edge systems, if compromised, could introduce new points of failure with potentially critical consequences regarding an application's confidentiality, availability, and integrity.

*Main Recommendation:* Cloud-edge systems should offer feasible redundancy for time-critical applications, monitoring, and real-life response capabilities. This can be bolstered with Digital Twin-type simulations of systems together with AI to identify and analyse potential effects of security events.

## 11.10. Data Storage and Collection

*Key Driver:* Data availability in distributed – in terms of geography and network topology – systems with regard to process performance, data collection/distribution, optimal network utilisation and ownership and control of the data.

*Main Recommendation:* European cloud-edge systems need open frameworks for data exchange and multi-orchestration to assure their uptake. To fully capitalize on the distributed nature of the edge-to-cloud continuum and the integration of sensors and existing data spaces, it should be accompanied by data marketplaces equipped with common, open metadata catalogues.

## 11.11. Scalability of Providers

*Key Driver:* To make cloud-edge systems a viable alternative to traditional clouds for European application providers, the ability to scale their operations is of paramount importance. It is not only a technological challenge (discussed in section 9) but also a market one.

*Main Recommendation:* Establish channels of communication between providers and users that will raise "application awareness" in the cloud-edge infrastructure, thus limiting the risk of inadequate resource allocation to fulfil the functional and additional requirements of the service. Secondly, follow industry standards and leverage mature open source solutions.

## 11.12. Ecosystems Integration

*Key Driver:* A tighter partner ecosystem integration will be required since not only the deployment but also day-to-day operations must be orchestrated.

*Main Recommendation:* Resilience concepts for service continuum need to be developed that include processes for proactive notifications, service recovery, and other capabilities. While the level of integration must be increased, cost must be driven down.

## 11.13. Energy Consumption

*Key Driver:* To leverage optimisation of energy supply and reuse waste energy we must integrate edge cloud deployments with other elements such as solar energy, hydrogen energy solutions, energy storage, etc., and with installations that can utilise excess energy such as horizontal gardening and district heating.

*Main Recommendation:* In the urban development plans there must be inclusive project approaches that make integration and synergies a priority and include the overall net effects in their business cases.

## 11.14. Coordination and Definition of Standard Interfaces and APIs

*Key Driver:* Historically, interfaces and APIs are highly vendor dependent as this is the domain of the vendor. This is the area where vendors implement their 'vendor lock-in' strategies and where they can dictate features as well as price.

*Main Recommendation:* A major challenge is to coordinate all stakeholders of the different interfaces and APIs and promote the use of alternative standards.

## 11.15. Open Source Innovation Model

*Key Driver:* Many companies still do not fully understand the way in which producing open source software and retaining IP rights is compatible, which leads to some technology providers being reluctant to either publish some of their assets or to contribute to external collaborative open source projects.

*Main Recommendation:* Find ways to educate companies to support open source and to understand its innovation model (which sometimes involves technical collaboration with traditional competitors), and the opportunities it brings to open up new business areas without compromising their IP.

## 11.16. Open Source Adoption

*Key Driver:* Some companies and public organisations are still reluctant to adopt open source technologies.

*Main Recommendation:* Define a Europe-wide plan to promote the benefits of open source and the role that innovation around open standards and open source technologies is expected to play in Europe's next-generation edge cloud and in the data economy.

# ANNEX: OPPORTUNITIES & CHALLENGES OF DIGITAL SOVEREIGNTY

## Landscaping Sovereignty-Enabling Building Blocks

### Digital Sovereignty

The Alliance for Industrial Data, Edge and Cloud ('Alliance') focuses on fostering the joint development and deployment of next-generation EU native cloud, edge and far edge (IoT) technologies. This initiative, in line with the EU Fit for the Digital Age, Digital Decade 2030 targets, EU data strategy, cybersecurity strategy and related strategies, meets the requirements to process Europe's sensitive personal data and non-personal data as well as sensitive business and public sector data sets, by addressing use cases for all sectors of the economy, with a specific focus (although without limitation) on defence, security, mobility, health, and space. The vision and mission are further described on the Alliance's website [1], and in its Terms of Reference [177].

Digital data makes a crucial cornerstone of the 2030 Digital Decade policy programme. It is the common denominator, and according to the targets in the 2030 Digital Decade:

- 75% of EU enterprises will use computing services, big data or AI.
- Europe will grow the pipeline of its innovative scale ups and improve access to finance, leading to the number of unicorns doubling.
- 100% of key public services for citizens and businesses will be available online.
- 100% of European citizens will have access to electronic health records.
- 80% of citizens will have access to a digital ID solution.

The increasing use of data processing and related computing technologies such as cloud, edge, and far edge computing, is promoting and enabling data exchange, but operation and implementation do not generally meet the minimal threshold of digital sovereignty and are not yet regulated by formal and standardised policies. In line with the EU Data Strategy, data processing technologies, hosted on cloud, should ultimately enable, facilitate, and sustain the development and implementation of European data spaces, where multiple economic sectors are involved.

The merger of information technology and operational technology with communication technology, and related migration from traditional infrastructures to cloud platforms, has led to the acquisition, build-up, and concentration of data by a relatively small group of organizations. The effect of this is widespread, from private users' data to that of organizations (public, private, and otherwise), and it generates economic, personal and other societal uncertainty around important aspects such as security, safety, privacy, data, data flows (whether personal or non-personal) and trust at large, in this digital age.

To mitigate this trend, numerous EU initiatives have been created to develop tools and best practices to regulate the use of data, its transfer and cross-border exchange, as well as ensuring its security. Additionally, there are EU projects promoting open strategic autonomy in general and digital sovereignty as main prerequisites.

More generally the need for Digital Sovereignty is linked to the growing concern that the citizens, businesses, and administrations of the Member States of the European Union are gradually losing control over their data, their capacity for innovation and technological development, their ability to shape and enforce legislation in the digital environment, and access to hardware and software technologies and capabilities. Support has been growing for a new policy approach designed to enhance Europe's strategic autonomy in the digital field with the objective of protecting the EU values and human rights and strengthening the position of the EU economy.

### Omnipresence of Digital Sovereignty

Digital sovereignty is an omni-present dimension. It is relevant:

- *during the entire lifecycle* of the systems, the data, and any data processing
- *before and during strategic* venturing, partnering, investing in knowledge, talent, cash and kind, and other collaborations
- before and during *procurement, sourcing, development, production, integration, building and implementation*
- before and during *deployments and ongoing operations and upgrading*
- during *scheduled and unscheduled events* and maintenance, incidents, attacks by malicious actors, recovery, further hardening and improvements
- when preparing for and implementing any *re-use, switching, recycling, up-cycling or decommissioning*.

Digital sovereignty creates, identifies, defines, loads and otherwise nuances a vast set of notions, principles, dimensions, perspectives and other related requirements to achieve the appropriate digital sovereign levels of data processing and related data processing infrastructures in Europe aimed by the Alliance.

### Building Blocks

Cloud, edge, and far edge technologies, infrastructures, and capacities are the basis of the European digital transformation of industry, society, and public administration for the benefit of citizens and undertakings. Moreover, they can help to achieve EU sustainability objectives. As a consequence, the development in Europe of cloud and edge capabilities should pursue greater EU strategic digital autonomy, aiming to keep pace with other countries that are leaders in some areas.

EU digital sovereignty can be defined as Europe's ability to act independently in the digital world and is related to the capacity of maintaining control of the products, systems, and services with any digital elements used by European citizens, undertakings, and public administrations. The

meaningful control over the technological components and elements thereof should include the different phases including the design, production, operation, use, improvement, sustainment and resilience, throughout their entire life cycles.

Digital components are largely dominated by non-EU companies and for the purpose of technical sovereignty for edge and cloud it is useful to consider:

- Hardware level including:
  - Chips (e.g. semiconductors: computing, power management)
  - Boards (aggregation of chips)
  - Devices/apparatus (e.g. connectors, routers, computers, switch, smartphones, embedded subsystems, and other components)
- Software level including:
  - Embedded software
  - Basic operating software (e.g. operating system, cloud infrastructure software)
  - Application-related software (e.g. database management)
- Data including:
  - Actual data
  - Meta data related to actual data
  - Inferenced data (from actual data and metadata)
- Infrastructure topology taking into consideration centralised and distributed architectures towards edge and far edge.

In order to grasp the various notions, principles, dimensions, perspectives and other related requirements, and create certain oversight and insight, it is essential to landscape the most relevant sovereignty-enabling building blocks.

These building blocks have different shapes and sizes, are n-dimensional, contextual, principle-based and dynamic, and they need to be combined, configured, monitored and kept up to date. This, together with the aim that the applicable blocks can be combined and used in an appropriate way to architect, design, manufacture, provide, procure, and sustain a holistic, hybrid, end-to-end, ecosystem of ecosystems, mission-based, layered symbiosis of digital sovereign data processing in the European Union. System-thinking, and system-doing are the essential notions to both start from, and from which to validate any initial or other architecture, implementation plan, deployment, etc.

### Neutral & Agnostic

Digital sovereignty could be the subject of an entire book series. Therefore, this section does not claim to be exhaustive. It is, however, useful to provide certain oversight and insight, as well as to provide certain guidance on principles, requirements, and recommendations for the members of the Alliance – both public, private and otherwise. This, in whatever technical, technical-

organizational, organizational or governance layer, domain or dimension one is mostly focusing on. This guidance is deemed to be technology-neutral, vendor-neutral, and otherwise agnostic.

Furthermore, this guidance should not monopolize in any way the various definitions of digital sovereignty, as this truly depends on the individuals, their position, location, and situation. For instance, in various workshops and other sessions with the taskforce that is made up of members from the private sector, the term 'data sovereignty' was highlighted and discussed multiple times.

### Seeking Perspective as First Step

There are many ways of segmenting digital sovereignty.

The first essential in the steps towards grasping identity and work on digital sovereignty is *perspective*. The second essential is *context*, the third is *stakeholder plotting and mapping*, and the fourth is *having a multi-angled, value-based, risk-based, and overall impact-based approach*. This, as digital sovereignty is the net outcome of both freedom and joint-freedoms, responsibilities, and joint-responsibilities, and balancing these out, before, during and after design, implementation, procurement, deployments, and use.

### Connectivity Level

When starting from the perspective of a holistic, high level, end-to-end ecosystem approach, an initial segmentation can be done in four segments, as outlined below:

- *Non-connected*, which can be a stand-alone device, tool, machine, appliance, application, or data source that does not have connectivity that can connect to, for instance, the internet, local or other networks / resources.
- *Connected*, where a device, tool, machine, appliance, application, data source, or system may be connected via the internet to local networks, centralised or decentralised computing infrastructures, networks, or other resources.
- *Inter-connected*, where several edge devices, tools, machines, appliances, applications, data sources or systems are connected with each other, either via orchestrated or federated systems.
- *Hyper-connected*, where numerous far-edge and other IIoT devices, tools, machines, appliances, applications, data sources or systems are directly connected with each other via distributed and otherwise fragmented ecosystems of ecosystems.

The fifth segment would obviously be combinations and variations of the first four segments.

### X-Centricity

When starting from the perspective of x-centricity approach, an initial segmentation can be done as follows: one should focus initially on the various dimensions – People, Organizations, Personas and Data – that in one or more ways than in the other are relevant in all or most of the technical layers respectively service-oriented ecosystems:

- Human & People-centric
- Stakeholder-centric
- Persona, Identity, Authentication & Authorization-centric
- Data & Attribute-centric
- Data source-centric

as well focusing on the applicable technical domains:

- Network & Communication-centric
- Infrastructure-centric
- Computing-centric
- Application & Platform-centric
- Hardware or Device-centric
- Services-centric

Other, subsequent x-centricity segments would obviously be combinations and variations of the dimensions and layers mentioned above, merged into:

- System-centric
- Supply-chain-centric
- Community-centric
- Societal-centric
- Economic-centric
- Ecological-centric

These holistic-centric perspectives are quite essential, as having meaningful control over only one technical layer or one dimension does not equal digital sovereignty.

### Meaningful Control

The notion of meaningful control is used in this section as it is agnostic. This approach is necessarily in the domain of digital sovereignty. For example, one may believe one has meaningful control by means of having an SOC or by means of an SLA, but that does not empower one to be sufficiently and factually prepared and ready to discover and make strategic decisions to address (A) the future mode of operation, (B) how to respond to threats, (C) a change of control of the data processor or other essential provider, supplier or vendor. Also, when one has all these measures in place with a key vendor, what about the other direct or indirect suppliers or stakeholders upstream or side-stream in the relevant ecosystems?

### Add Other Perspectives

The examples of segmentation above are obviously not the only ones possible. Various other segmentations are to be considered, such as real-time or near-real-time functionalities. This segmentation may be relevant when near-real-time autonomous functionalities and capabilities are considered (in mobility, defence, security, or elsewhere), or real-time prognostic health monitoring

or related integrated logistics support are relevant (in mobility, defence, security, vital or near-vital infrastructures and supply chains, or elsewhere). Other segmentations that can be considered are, for instance, single-vendor, multi-vendor, OEM, public, private, public-private, etc.

### Status Quo or Digital Transformation

As an example of the second essential in the steps towards grasping, identifying and working on digital sovereignty, namely: *context*, the segmentation can be the following:

- *Legacy:* Systems, processes, data, data flows, data processing, governance, and creating oversight, insights and other transparency in order to be able to assess if and to what extent one has meaningful control and digital sovereignty in any scenario.
- *Retrofit & Redesign:* Which of those legacy components, layers, processes, dimensions, or policies have the capability to improve towards achieving and sustaining meaningful control and other digital sovereignty characteristics in any scenario?
- *Design & Greenfield:* Systems, processes, data, data flows, data processing, governance designed with the resilient and otherwise future-proof capability to building and sustaining digital sovereignty in any scenario.
- *Digital Transform:* Which of the legacy components, layers, processes, dimensions or policies can be down-ramped after the new ones have proven to be operating as envisioned and designed and are up-ramped thereafter, and which new ones can be seen as greenfield without being hampered by legacy?

### Life Cycle Thinking and Doing

When approaching sovereignty, it is crucial to assess the boundaries of the use case and its requirements in terms of the data and information that will be handled and processed so to pick the correct sovereignty framework and apply it to the whole life cycle. Looking at the digital system as a whole, each of its components needs to be assessed in terms of how long a connected device, product, system and service can or needs to remain connected to digital ecosystems in a secure, safe, trustworthy, and compliant manner.

In terms of data, at each phase of the life cycle, relevant stakeholders must be identified and their access to and accountability for the data itself, metadata, and inference data must be clearly stated and regulated. In this context, data classification becomes more and more central as well as classification updates over time.

From a technical standpoint, technologies such as Hold Your Own Key (HYOK), Privacy-enhancing Computation (PEC), Confidential Computing can enable a sovereign compliant use, process and storage of data and even its true deletion.

In order to account for the whole life cycle, topics such as perpetual use of software and services and migration services to avoid lock-in issues must be addressed so the end user is aware of them.

Furthermore, maintaining compatibility and maximum feature parity with public clouds allows the running of workloads across a spectrum of sovereignty (from low to high) in a seamless way.

This lifecycle thinking / doing is another example of the second essential and towards digital sovereignty – *context*. It includes segmenting one or more technical layers, dimensions (such as data) and the (eco)systems these are part of, per lifecycle phase. This, as verifying and assuring digital sovereignty in one particular life cycle phase, is essential, but it does not equal digital sovereignty in the next life cycle phase let alone further down the road or in the entire life cycle. Alongside the examples provided above, one can for instance think about the various dynamics that are part of every life cycle, including those of digital systems, devices, stakeholders, context, legal relationships and data, for instance:

- *Digital Systems Life Cycle:* What does the life cycle entail; how long can or does a connected device, product, system and service need to remain connected to digital ecosystems in a secure, safe, trustworthy, and compliant manner; what can customers, users, and society expect; how are the parts of the ecosystem and users/customers able to keep up to date with the state of art?
- *Stakeholders' Life Cycle:* What stakeholders are involved regarding a device, product, system, or service and in a relevant ecosystem, what if the dynamics thereof change; who is accountable for which part of the ecosystem; how to keep the stakeholders up to date; what happens if there is an incident within the digital ecosystem of any kind or size?
- *Data Life Cycle:* What data is collected, created, or otherwise concerned; what is its classification; can it be segmented, minimised and isolated; what if it has multiple classifications; what if the classification changes; who controls the data; for what purposes is one entitled to process the data; what meta data and derived data is generated during the data life cycle; with whom is data or certain attributes thereof shared; what does true data deletion mean?
- *Contextual Life Cycle:* In what context is a device/product/(eco)system used; as which persona is a stakeholder involved; in what context is data used; what if this context changes; who is accountable in which context; how to make stakeholders aware of changes in best practices, rights, and obligations when the context changes; how to secure the rights and obligations of the relevant other stakeholders?
- *Legal Life Cycle:* As an organization or person, with whom does one need to engage; how to assess, prepare, negotiate, contract, execute, operate, update, amend, escalate and terminate such engagement (being a combination of contractual, regulatory and other legal relationships)?

### Intertwined Domains

The penultimate segmentation for landscaping sovereignty-enabling building blocks and making those deployable are the ones which can already be found in the relevant strategies by the Commission, including the Data Strategy, Cybersecurity Strategy, Digital Decade 2030 Objectives

and Targets, and its Declaration on Digital Rights and Principles for the Digital Decade, to name a few. A way to segment those is to define four domains, set forth below in random order:

- Research & Innovation
- Education, Skills & Jobs
- Economic Development & Competition
- Collaborative Resilience

These four main domains are contextual, impact-based and, most of all, intertwined.

### Sovereignty layers

According to Gartner's analysis [178], sovereignty can be segmented in five layers of need that must be met with cloud capabilities and commitments:

- *Privacy layer*: focuses on data and on data owners who claim rights to that data. In this context, a sub-layer of protection can be identified which keeps the data safe and where it is possible to visualize the data location and access
- *Residency layer*: addresses the need for data be moved according to specific rules and processes and to be confined within a geopolitical boundary when at rest
- *Locality layer*: it is a technology that needs to be physically located within a geopolitical boundary, so that no part/component of the technology is located elsewhere
- *Authority layer*: controls who can make decisions regarding cloud at large, including services and application, infrastructure, and platform components and assets
- *Ownership layer*: legal boundaries of ownership of services and application, infrastructure, and platform components and assets

### Timelines

The final segmentation for landscaping sovereignty-enabling building blocks and making those deployable is the dynamics perspective. Where the only constant is change, regarding digital sovereignty one needs to think and act in all phases, including all phases from extreme short term to extreme long term.

The above notions, including the various sovereignty-enabling building blocks these create, interconnect, put into use and make operational with the mission of the Alliance have already been explained in the various priorities in the Roadmap, notably in Section 2 on sovereignty and Section 4 on cybersecurity.

# Building, Achieving and Sustaining Digital Sovereignty

### Holistic Approach to Digital Sovereignty

In an increasingly globalized world, Europe presents itself as a champion of ethical values but cannot yet guarantee the digital sovereignty of its citizens or its businesses. Answering the question on how to build, achieve, and sustain European digital sovereignty is not an easy feat.

When discussing any roadmap and mini-roadmaps in this digital age, it is necessary to take a holistic approach being in mind the overall aim of European digital sovereignty, and – as private sector, public sector, and society at large within the EU – to be co-responsible for enabling, facilitating, building, achieving, and sustaining it. For this, it is not enough to focus on the technological aspects (i.e. technological sovereignty) and to keep in mind the other dimensions and the interdependencies between them. For example, research and innovation can only be achieved with strong digital competencies (i.e. education and skills) and investments (i.e. economics and investment).

The general aim of this Roadmap is to both identify and jointly work on addressing, mitigating (and even solving) the challenges regarding European digital sovereignty in a technically, organizationally, socially, ecologically, and economically feasible and sustainable way, overcoming fragmentation while identifying and joining European brainpower and forces to build, boost, and amplify the gains of (the road towards) building, achieving, and sustaining European digital sovereignty. The main concepts behind each of the layers of sovereignty outlined in the previous section can be summarized as follows.

- Data Control, Data Access, Data Use & Data Protection (Data Rights)
    - Operators can neither access nor view the data
    - HYOK: encryption keys held solely by the client
    - Audits on data and governance must comply with local privacy regulations per jurisdiction
    - Data compliance with local/regional regulations (e.g. GDPR)
    - Compelled access by external authorities is avoided
- Residency (Movement and Rest)
    - Services running in jurisdiction
    - Data at rest stored only in jurisdiction
    - Client data storage must be specific and specified
    - Client can appeal and request sanctions for non-agreed data movement
    - Agreed data movement tracked and documented
    - Line of sight between accountable sides
    - Edge/cloud local interfaces
- Locality Layer (Physical Location)
    - End-to-end local data transfer

    - Cloud infrastructure (tenants, storage) run locally
    - Set of cloud services delivered in an isolated (potentially air-gapped) fashion
    - Control plane under local jurisdiction
    - Action enforcement in charge of partners
    - SLA and support managed locally
- Authority Layer (Decision Rights):
    - Security certification at a country/regional level
    - Data subjected to local legal jurisdiction
- Control & Governance Layer (Ethical, Governance & Legal Rights):
    - Infrastructure and services have local or governmental owners or controller
    - These owners or controllers can grant local governance requirements
    - Decisions are taken at a local level
    - Authority must be independent from outside influence

### Dependability

All organizations across the globe, regardless of their sector, have to adapt to the new digital challenges. This means acting to implement state-of-the-art security in both cyber and physical domains, focusing on safety, implementing accountability in both technical and organizational aspects, protecting privacy and data, cyber resilience and transparency.

This leads to various challenges to address, risks to mitigate, impact to avoid, scenarios to prepare for, re-organize or otherwise coordinate and orchestrate detrimental consequences and related responsibility, accountability, liability, and enforcement capabilities, as well as renewed or otherwise improved monitoring and supervising in this digital age. While the existing policy instruments, the efficiency of governmental authorities, as well as existing legal structures, responsibilities, measures, remedies, and other capabilities are challenged, these are – as they improve and become more transparent and accountable – certainly also part of the solution.

### Opportunities & Challenges of Digital Sovereignty

The challenges and dilemmas of digital sovereignty and the notion of constant change and related dynamics also lead to many different opportunities to identify, seize, embrace, incentivize and organize, support, augment, and expand digital sovereignty. As discussed above, we need to be flexible and ready to accept changes round the clock if we want to mitigate the continuously evolving challenges, and this point is forcing us to rethink and design a policy which can help us to address this and remain valid in the ever-evolving dynamics of the current digital age. Static instruments in a dynamic digital and cyber-physical world will generally no longer be up to the job they were intended and designed for.

# Bridging the Resourcing Gap

### How to Cater for Digital Sovereignty, Now and in the Future

This paragraph briefly mentions only one of the many objectives and challenges involving digital sovereignty, which is how to bridge the resources gap, for instance concerning European research, innovation, education, skills, jobs, economic development, competition, and collaborative resilience that help to cater for digital sovereignty, in the extreme-short, short, mid, long, and extreme-long term.

### Investments & Commitments

To bridge the resources gap is not merely a matter of funds and the access to funds. The ability of the public sector (one of the major purchasers and users of digital services, systems, and devices) to purchase items from European markets that are willing to invest in digital sovereign devices, systems, and services, including but not limited to data processing in the appropriate computing continuum spectrum with the appropriate process, is one way to bridge the resources gap.

### Skills & Competencies

To bridge the resources gap is not merely a matter of more students passing their exams based on traditional curricula. National governments or other organizations that decide on national curricula must also be willing to include digital sovereignty issues, thinking, and doing, including without limitation IT ethics, non-functionals, and accountability - and most definitely not just at university level.

In this case, bridging the resources gap is about making education more interoperable on the skills needed in this digital age, where the EU public and private sector should be willing to invest in those skilled persons, and make sure they have jobs with many learning curves and prosperity ahead. Demography-wise, the EU and its Member States already have challenges but these will increase in the next decades. This is another reason to start working and collaborating on this today. Any market only starts and works if all sides of the market are part of it and willing to engage.

# REFERENCES

[1] Cloud Alliance, https://digital-strategy.ec.europa.eu/en/policies/cloud-alliance

[2] European Data Strategy, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en

[3] Commission welcomes Member States' declaration on EU cloud federation, https://digital-strategy.ec.europa.eu/en/news/commission-welcomes-member-states-declaration-eu-cloud-federation

[4] Research and innovation at the heart of the new industrial strategy for Europe, https://research-and-innovation.ec.europa.eu/news/all-research-and-innovation-news/research-and-innovation-heart-new-industrial-strategy-europe-2021-05-05_en

[5] Digital sovereignty: Commission kick-starts alliances for Semiconductors and industrial cloud technologies, https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3733

[6] Industrial alliances: Commissioner Breton chairs first meeting of European Alliance for Industrial Data, Edge and Cloud, https://digital-strategy.ec.europa.eu/en/news/industrial-alliances-commissioner-breton-chairs-first-meeting-european-alliance-industrial-data

[7] European Industrial Strategy, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-industrial-strategy_en

[8] Cloud Computing Strategy, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF

[9] Joint Declaration on Next Generation Cloud, https://digital-strategy.ec.europa.eu/en/news/towards-next-generation-cloud-europe

[10] European Cloud Providers Continue to Grow but Still Lose Market Share, https://www.srgresearch.com/articles/european-cloud-providers-continue-to-grow-but-still-lose-market-share

[11] Eurostat, https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Cloud_computing_-_statistics_on_the_use_by_enterprises#Use_of_cloud_computing:_highlights

[12] Europe's Digital Decade: Commission sets the course towards a digitally empowered Europe by 2030, https://ec.europa.eu/commission/presscorner/detail/en/IP_21_983

[13] Open Source Observatory (OSOR), https://joinup.ec.europa.eu/collection/open-source-observatory-osor/news/thierry-breton-role-open-source

[14] Shaping Europe’s digital future, https://digital-strategy.ec.europa.eu/en/library/study-about-impact-open-source-software-and-hardware-technological-independence-competitiveness-and

[15] Standardisation Strategy, https://ec.europa.eu/commission/presscorner/detail/en/ip_22_661

[16] Green Deal, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/european-green-deal_en

[17] European industrial technology roadmap for the next generation cloud-edge offering, https://ec.europa.eu/newsroom/repository/document/2021-18/European_CloudEdge_Technology_Investment_Roadmap_for_publication_pMdz85DSw6nqPppq8hE9S9RbB8_76223.pdf

[18] Catena-X, https://catena-x.net

[19] White Paper on Manufacturing-X, https://www.plattform-i40.de/IP/Redaktion/EN/Downloads/Publikation/Manufacturing-X_long.html

[20] Smart connected supplier network, https://smart-connected.nl/en
[21] EONA-X, https://eona-x.eu
[22] Big Data Value Association, https://www.bdva.eu
[23] European Open Science Cloud, https://eosc.eu
[24] Gaia-X, https://gaia-x.eu
[25] Alliance IoT, https://aioti.eu
[26] IPCE-CIS, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52014XC0620%2801%292
[27] Data Spaces Support Centre, https://dssc.eu/
[28] European Data Centre Association, http://eudca.org
[29] EUCLIDIA, https://www.euclidia.eu
[30] Industrial Digital Twin, https://industrialdigitaltwin.org/en/
[31] ECLASS, https://eclass.eu/en
[32] OPC Foundation, https://opcfoundation.org
[33] GSMA Open Gateway, https://www.gsma.com/futurenetworks/gsma-open-gateway/
[34] tmforum, https://www.tmforum.org
[35] 5G Alliance for Connected Industries and Automation (5G ACIA), https://5g-acia.org
[36] OPEN Compute Project, https://www.opencompute.org
[37] European Commission Recommendation 2023/498 of 1 March 2023 on a Code of Practice on standardisation in the European Research Area
[38] The LINUX Foundation, https://www.linuxfoundation.org
[39] The LINUX Foundation in Europe, https://linuxfoundation.eu
[40] LF EDGE, https://www.lfedge.org
[41] Cloud Native Computer Foundation, https://www.cncf.io
[42] Eclipse Foundation, https://www.eclipse.org
[43] Edge Native Working Group, https://edgenative.eclipse.org
[44] Eclipse IoT, https://www.eclipse.org/org/workinggroups/iotwg_charter.php
[45] Apache Software Foundation, https://www.apache.org
[46] European Open Source for Europe's Next-Gen Edge Cloud, https://sovereignedge.eu
[47] Open Forum Europe, https://openforumeurope.org/open-source/
[48] O-RAN Alliance, https://www.o-ran.org
[49] OpenInfra, https://openinfra.dev/
[50] Introducing the next-generation operating model, https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/introducing%20the%20next-generation%20operating%20model/introducing-the-next-gen-operating-model.ashx
[51] Business Model Navigator, https://businessmodelnavigator.com
[52] Eclipse Data Components, https://github.com/eclipse-edc/Connector
[53] Digital product passports: enhancing transparency & consumer information, https://www.europarl.europa.eu/committees/de/digital-product-passports-enhancing-tran/product-details/20220510CHE10181
[54] ZVEI-Show-Case PCF@ControlCabinet (WhitePaper), https://www.zvei.org/presse-medien/publikationen/zvei-show-case-pcfcontrolcabinet-whitepaper
[55] Europe Fit for the Digital Age: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_en. Digital Decade 2030: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en.

[56] European Declaration on Digital Rights & Principles, EU's 'digital DNA', signed on 15 December 2022, and in force per January 2023, https://ec.europa.eu/commission/presscorner/detail/en/IP_22_7683, and the Digital Decade policy programme 2030 (DDPP 2030)

[57] Digital sovereignty for Europe, https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf

[58] Digital Decade 2030 Objectives: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age_en

[59] Digital Decade 2030 Targets: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en

[60] Hamm, A., Willner, A. and Schieferdecker, I. (2019). Edge Computing: A Comprehensive Survey of Current Initiatives and a Roadmap for a Sustainable Edge Computing Development, ArXiv https://doi.org/10.48550/arXiv.1912.08530

[61] Digital technology can cut global emissions by 15%. Here's how | World Economic Forum

[62] Climate Neutral Data Centre Pact, ClimateNeutralDataCentre.net

[63] The European Commission's Code of Conduct for Energy Efficiency in Data Centres, https://joint-research-centre.ec.europa.eu/energy-efficiency/energy-efficiency-products/code-conduct-ict/code-conduct-energy-efficiency-data-centres_en

[64] The European Green Digital Coalition, https://digital-strategy.ec.europa.eu/en/policies/european-green-digital-coalition

[65] 2021–2023 global supply chain crisis, https://en.wikipedia.org/wiki/2021%E2%80%932022_global_supply_chain_crisis

[66] European Automobile Manufacturers' Association (ACEA), COVID-19 impact on EU automobile production, https://www.acea.auto/figure/interactive-map-covid-19-impact-on-eu-automobile-production-first-half-of-2020/

[67] De Vet, J.M., Nigohosyan, D., Núñez Ferrer, J., Gross, A-K., Kuehl, S. and Flickenschild, M. (2021), "Impacts of the COVID-19 pandemic on EU industries", EU Parliament, Policy Department for Economic, Scientific and Quality of Life Policies, Directorate-General for Internal Policies.

[68] Hauschild, M.Z., Kara, S., Røpkec, I, (2020), "Absolute sustainability: Challenges to life cycle engineering", Elsevier CIRP Annals, 69(2), 533-553

[69] EFFRA, "MADE IN EUROPE - The manufacturing partnership in Horizon Europe", https://www.effra.eu/sites/default/files/made_in_europe-sria.pdf

[70] GRI and ISSB provide update on ongoing collaboration, https://www.globalreporting.org/news/news-center/gri-and-issb-provide-update-on-ongoing-collaboration/

[71] How Much Energy Do Data Centers Really Use?, https://energyinnovation.org/2020/03/17/how-much-energy-do-data-centers-really-use/

[72] Idata centre "Data Age 2025" White Paper, https://www.import.io/wp-content/uploads/2017/04/Seagate-WP-DataAge2025-March-2017.pdf

[73] H-Cloud White Paper, https://www.h-cloud.eu/?wpdmdl=4541&ind=1645025986562

[74] https://ec.europa.eu/finance/docs/level-2-measures/taxonomy-regulation-delegated-act-2021-2800-annex-1_en.pdf p179

[75] Climate Neutral Data Center, https://www.climateneutraldatacentre.net/

[76] Data Centres Code of Conduct, https://e3p.jrc.ec.europa.eu/communities/data-centres-code-conduct

[77] Li, W. et al. (2018), "On Enabling Sustainable Edge Computing with Renewable Energy Resources", IEEE Communications Magazine, 56(5), 94-101
[78] Performance per Watt, https://en.wikipedia.org/wiki/Performance_per_watt
[79] Sustainability Metrics, https://go.schneider-electric.com/WW_202111_WP67-Sustainability-Metrics-EN_MF-LP.html?utm_source=blog&utm_medium=banner&utm_campaign=cloudcolo
[80] HCloud Whitepaper Pillar 4 and Section 7.1.2 Hardware
[81] Cloud Security Alliance, "The State of Cloud Security in 2020", https://cloudsecurityalliance.org/articles/the-state-of-cloud-security-2020-report-understanding-misconfiguration-risk/
[82] SANS Institute, "Cloud Security: The Top 10 Risks for Cloud Computing", https://www.sans.org/media/cloud-security/eBook_cloud-security.pdf?msc=cloudsecuritylp
[83] NIST, "Cloud Security: A Comprehensive Guide"
[84] ENISA Working Group on "Security Operation Centres", https://www.enisa.europa.eu/login?came_from=/topics/cross-cooperation-for-csirts/ad-hoc-working-group-on-socs
[85] A.N. Toosi et al. (2014), "Interconnected Cloud Computing Environments: Challenges, Taxonomy and Survey", ACM Computing Surveys 47(1), 7, 1-47
[86] R. Buyya et al. (2019), "A Manifesto for Future Generation Cloud Computing: Research Directions for the Next Decade", ACM Computing Surveys 51(5),105, 1-38
[87] GridFTP data transfer protocol, https://docs.globus.org/
[88] Cloud Standards Customer Council, Cloud Interoperability and Portability Guide, https://www.omg.org/cloud/deliverables/CSCC-Interoperability-and-Portability-for-Cloud-Computing-A-Guide.pdf
[89] ETSI, Interoperability and Security in Cloud Computing, https://www.etsi.org/deliver/etsi_sr/003300_003399/003391/02.01.01_60/sr_003391v020101p.pdf
[90] NIST, Cloud Computing Standards Roadmap, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-291r2.pdf
[91] GSMA – Operator Platform Group, https://www.gsma.com/futurenetworks/5g-operator-platform/
[92] GSMA – Telco Edge Loud Forum https://www.gsma.com/futurenetworks/telco-edge-cloud-forum/
[93] Linux Foundation Announces New Project "CAMARA - The Telco Global API Alliance" with Global Industry Ecosystem, https://www.linuxfoundation.org/press/press-release/linux-foundation-announces-new-project-camara-the-telco-global-api-alliance-with-global-industry-ecosystem
[94] SYLVA Initiative, https://gitlab.com/sylva-projects/sylva
[95] Multi-Operator MEC POC, https://www.gsma.com/futurenetworks/wp-content/uploads/2021/03/5G-Live-Multi-Operator-MEC-POC-04.03.21.pdf
[96] Telco Edge Cloud Trial – Bridge Alliance Federated Edge Hub and MobiledgeX Interconnection, https://www.telefonica.com/en/communication-room/bridge-alliance-mobiledgex-singtel-and-telefonica-achieve-world-first-interconnection-of-heterogenous-multi-access-edge-computing-mec-platforms-utilising-hub-to-hub-architecture/
[97] Anuket Linux Foundation, anuket.io
[98] IPCEI-CIS Project of Common European Interest for the Next Generation Cloud Infrastructure and Services, https://www.bmwk.de/Redaktion/DE/Downloads/I/ipcei-cis-value-chain-description.pdf?__blob=publicationFile&v=8
[99] Gartner, https://www.gartner.com/en/newsroom/press-releases/2021-11-01-gartner-predicts-half-of-cloud-data-centers-will-deploy-robots-with-ai-capabilties-by-2025

[100] HIPEAC VISION 2023, https://www.hipeac.net/vision/2023.pdf
[101] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A European strategy for data, Brussels, February 2020, https://digital-strategy.ec.europa.eu/en/policies/strategy-data
[102] IDC, "A Blueprint for DX Success: Start with Hybrid Infrastructure and Connected Ecosystems", https://www.equinix.in/resources/analyst-reports/dx-success-hybrid-infrastructure-connected-ecosystems
[103] GSMA, "The Mobile Economy 2022", https://www.gsma.com/mobileeconomy/wp-content/uploads/2022/02/280222-The-Mobile-Economy-2022.pdf
[104] IDG Communications, Network World, "3 Essentials for Achieving Resiliency at the Edge", https://www.networkworld.com/article/3386438/3-essentials-for-achieving-resiliency-at-the-edge.html
[105] Zero-touch network and Service Management (ZSM); Means of Automation. ETSI-ZSM. ETSI GR ZSM 005, https://www.etsi.org/deliver/etsi_gr/ZSM/001_099/005/01.01.01_60/gr_zsm005v010101p.pdf
[106] GSMA Operator Platform Telco Edge Requirements. GSMA OP.02 v3.0, https://www.gsma.com/futurenetworks/wp-content/uploads/2022/10/Operator-Platform-Telco-Edge-Requirements.-v.3-October22.pdf
[107] CAMARA Project, https://github.com/camaraproject
[108] Katsis et al (2022), "Edge Security: Challenges and Issues", https://arxiv.org/pdf/2206.07164.pdf
[109] Slalmi, Chaibi et al (2020), "On the Ultra-Reliable and Low-Latency Communications for Tactile Internet in 5G Era", Procedia Computer Science. Vol. 176,
[110] Leyva-Pupo, Irian, Alejandro Santoyo-González, and Cristina Cervelló-Pastor, (2019), "A Framework for the Joint Placement of Edge Service Infrastructure and User Plane Functions for 5G", Sensors 19, no. 18: 3975
[111] 3GPP, "5G System; Network Exposure Function Northbound APIs; Stage 3", TS 29.522, Release 17, 2022
[112] Ordonez-Lucena, Jose, Pablo Ameigeiras, Luis M. Contreras, Jesús Folgueira, and Diego R. López, (2021), "On the Rollout of Network Slicing in Carrier Networks: A Technology Radar" Sensors 21, no. 23: 8094
[113] I. Leyva-Pupo, C. Cervelló-Pastor, C. Anagnostopoulos, D.P.Pezaros, (2022), "Dynamic UPF placement and chaining reconfiguration in 5G networks", Elsevier Computer Networks, Volume 215
[114] RedHat, "What does an API Gateway do?", https://www.redhat.com/en/topics/api/what-does-an-api-gateway-do
[115] RCR Wireless News, "A 5G Standalone core will support advanced use cases and an open network architecture", https://www.rcrwireless.com/20211209/5g/a-5g-standalone-core-will-support-advanced-use-cases-and-an-open-network-architecture
[116] GSMA Operator Platform, https://www.gsma.com/futurenetworks/5g-operator-platform/
[117] ETSI-MEC Multiaccess Edge Computing; Framework and Reference Architecture, https://www.etsi.org/deliver/etsi_gs/MEC/001_099/003/03.01.01_60/gs_MEC003v030101p.pdf
[118] MEF Life-cycle Service Orchestration, https://wiki.mef.net/pages/viewpage.action?pageId=56165271
[119] 3GPP Enabling Edge Computing Applications, https://www.3gpp.org/news-events/3gpp-news/edge-sa6

[120] Credit Suisse, "Metaverse: A Guide to the Next-Gen Internet", https://www.credit-suisse.com/media/assets/corporate/docs/about-us/media/media-release/2022/03/metaverse-14032022.pdf

[121] Telecom Infra Project, "Open Transport SDN Architecture", https://cdn.brandfolder.io/D8DI15S7/at/jh6nnbb6bjvn7w7t5jbgm5n/OpenTransportArchitecture-Whitepaper_TIP_Final.pdf

[122] Telecom Infra Project, Open Optical and Packet Transport project group, https://telecominfraproject.com/oopt/

[123] Telecom Infra Project, telecominfraproject.com

[124] KDDI, Vodafone, MTN, Telefonica release disaggregated router requirements, https://telecominfraproject.com/kddi-vodafone-mtn-and-telefonica-to-drive-open-and-disaggregated-solutions-for-ip-core/

[125] IncreaseBroadbandSpeed, "TV and Video Will Triple Average Home Monthly Internet Usage to Beyond 1 TB By 2025", https://www.increasebroadbandspeed.co.uk/average-home-monthly-internet-usage-forecast

[126] Lorincz, Josip, Antonio Capone, and Jinsong Wu, (2019), "Greener, Energy-Efficient and Sustainable Networks: State-Of-The-Art and New Trends" Sensors 19, no. 22: 4864

[127] "2 European companies (Ericsson and Nokia) are in the Top 5 of 5G technology providers, both in terms of patents and revenues" in "Top 10 Companies leading the 5G Network Industry", Emergen Research, https://www.emergenresearch.com/blog/top-10-companies-leading-the-5g-network-industry

[128] "Top 5 European telecom operators serve close to 1,2 billion customers worldwide spread across the 4 main continents", GSMA Intelligence, https://www.gsma.com/mobileeconomy/wp-content/uploads/2022/10/051022-Mobile-Economy-Europe-2022.pdf

[129] It is expected that starting from 2023 ARM technology will increase the market share: https://www.nextplatform.com/2021/05/11/amd-finally-breaks-the-10-percent-server-share-barrier/

[130] None of the top-10 tech hardware companies is EU based: https://www.investopedia.com/articles/investing/012716/worlds-top-10-hardware-companies-aaplibm.asp

[131] Arduino, https://www.arduino.cc

[132] Rashberry Pi, https://www.raspberrypi.org

[133] OPEN 19, https://www.open19.org

[134] TELECOM INFRA Project https://telecominfraproject.com/

[135] Many hardware vendors include already OCP slots – which were defined by TIP – in their mainstream servers and other data centre equipment, e.g.: Dell: https://dl.dell.com/manuals/common/dell-tech-dfd-collab-contribute-ocp-nic-3-0.pdf, Lenovo: https://lenovopress.lenovo.com/lp0765-networking-options-for-thinksystem-servers, HPE: https://www.hpe.com/us/en/insights/articles/the-open-compute-project-not-just-for-servers-anymore-1805.html

[136] RISC-V, https://riscv.org

[137] Balthazar, a Personal Computing Device, One Laptop for the New Internet. https://balthazar.space/wiki/Balthazar

[138] V-One PCB printer, https://www.voltera.io/v-one

[139] Pen Source Hardware for Science and Beyond, https://commission.europa.eu/system/files/2021-11/javierserrano_osm_12_2018.pdf
[140] White Rabbit, https://commission.europa.eu/document/download/273c5429-122e-46c1-8a06-7eaad4259b2e_en
[141] Silicon, https://developers.google.com/silicon
[142] Opticians today have CNC milling machines for adapting the glasses (e.g.: https://www.fw-haug.com/fileadmin/media/downloads_list/S-614.pdf), dentists create tooth crowns directly in their dental practice (e.g., https://www.tools4cadcam.de/de/3d-druck/3d-drucker/)
[143] Techtarget, Cluster management and dependencies, https://www.techtarget.com/searchcloudcomputing/definition/cloud-management
[144] Intel, Chipset software, https://www.intel.com/content/www/us/en/support/articles/000005974/software/chipset-software.html
[145] OpenSSL, https://www.openssl.org
[146] Advanced Encryption Standard, https://www.nist.gov/publications/advanced-encryption-standard-aes
[147] AMD Memory Encryption, https://www.kernel.org/doc/html/v5.8/x86/amd-memory-encryption.html
[148] Confidential Computing concepts, https://cloud.google.com/compute/confidential-vm/docs/about-cvm
[149] European Coordination and Support Action in Cryptology, https://cordis.europa.eu/project/id/645421
[150] HORIZON-CL3, in https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/wp-call/2023-2024/wp-6-civil-security-for-society_horizon-2023-2024_en.pdf
[151] HORIZON-CL4, https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/wp-call/2023-2024/wp-7-digital-industry-and-space_horizon-2023-2024_en.pdf
[152] 6G SNS, https://smart-networks.europa.eu/wp-content/uploads/2022/10/snsriworkprogramme20212022_ckvqrabs7gkb08dhgl6wh73cwqa_82061-6.pdf
[153] Google Cloud, https://cloud.google.com/storage-transfer/docs/source-amazon-s3
[154] GSMA Federation (East-Westbound Interface) API, https://www.gsma.com/futurenetworks/resources/platform-group-4-0-federation-api-1-0-0-yaml/
[155] European Commission, Open source software strategy, https://commission.europa.eu/about-european-commission/departments-and-executive-agencies/informatics/open-source-software-strategy_en
[156] SONiC was developed by Microsoft and OCP. As the base operating system Debian is used, https://github.com/sonic-net
[157] CNCF Cloud Native Interactive Landscape, https://landscape.cncf.io/
[158] Statista, https://www.statista.com/statistics/1295999/update-frequency-top-ios-apps-by-category/
[159] PRNewswire, "30 percent increase in elite performers: Nagarro State of DevOps Report 2022", https://www.prnewswire.com/news-releases/30-percent-increase-in-elite-performers-nagarro-state-of-devops-report-2022-301725680.html
[160] Gartner, 2022-2024 Technology Adoption Roadmap for Midsize Enterprises, https://www.gartner.com/en/publications/technology-adoption-roadmap-for-midsize-enterprises

[161] Leonardo Project, https://www.ilsole24ore.com/art/al-cineca-bologna-arrivano-primi-tir-i-pezzi-supercomputer-leonardo-AEctTYoB?refresh_ce=1
[162] Petrosyan D, and Astsatryan H, (2022), "Serverless High-Performance Computing over Cloud", Cybernetics and Information Technologies, 22(3) 82-92
[163] Weka, GPU Acceleration for High-Performance Computing, https://www.weka.io/blog/gpu-acceleration/
[164] Frontiers of Engineering, "Reports on Leading-Edge Engineering", 2018 Symposium, https://nap.nationalacademies.org/catalog/25333/frontiers-of-engineering-reports-on-leading-edge-engineering-from-the
[165] Angel, Nancy A, Dakshanamoorthy Ravindran, P M Durai Raj Vincent, Kathiravan Srinivasan, and Yuh-Chung Hu, (2022), "Recent Advances in Evolving Computing Paradigms: Cloud, Edge, and Fog Technologies" Sensors 22, no. 1: 196
[166] Quantum Technologies, https://www.capgemini.com/wp-content/uploads/2022/03/Final-Web-Version-Quantum-Technologies.pdf
[167] European Commission, Blockchain Strategy, https://digital-strategy.ec.europa.eu/en/policies/blockchain-strategy
[168] ONTOCHAIN, https://ontochain.ngi.eu/
[169] European Commission, EBSI Architecture, explained, https://ec.europa.eu/digital-building-blocks/wikis/download/attachments/447687044/%28210610%29%28EBSI_Architecture_Explained%29%28v1.02%29.pdf
[170] International Data Spaces Organisation, https://internationaldataspaces.org
[171] MyData, https://www.mydata.org
[172] A New Governance, https://www.anewgovernance.org
[173] FIWARE, https://www.fiware.org
[174] GAIA-X, https://gaia-x.eu/use cases
[175] Sharing Europe's Digital Feature, https://digital-strategy.ec.europa.eu/en/news/simpl-cloud-edge-federations-and-data-spaces-made-simple
[176] FAIR Principles, https://www.go-fair.org/fair-principles/
[177] European Alliance for Industrial Data, Edge and Cloud, https://ec.europa.eu/newsroom/dae/redirection/document/78363
[178] Gartner, "How Can Hyperscale Cloud Providers Address the Growing Dilemma of Cloud Sovereignty"