


European industrial technology roadmap for the next generation cloud-edge offering

MAY 2021



This report is addressed to Thierry Breton, European Commissioner for the Internal Market. It was elaborated following the CEO Roundtable “Shaping the Next Generation Cloud Supply for Europe” that took place on 16 December 2020.

Prepared by:

AIRBUS

amadeus

aruba.it

Atos

Capgemini

CloudFerro

DE CIX

ERICSSON

gigas

**GERMAN
EDGE CLOUD**

indra

IONOS

IRIDEOS

leaseweb

**Magic
Cloud**

NabiaX

NOKIA

orange™

OUTSCALE

OVHcloud™

RETELIT

SAP

**Schneider
Electric**

SIEMENS

T. . .

Telefónica

TIM

Contents

Contents	3
Executive Summary.....	5
Glossary	8
Introduction	9
1. Context	10
1.1. Where are we now?.....	10
1.1.1. Strengths & opportunities	10
1.1.1.1. A dense and technologically diverse ICT industrial base	10
1.1.1.2. Globally recognized standards and open innovation culture	11
1.1.1.3. Opportunities to leverage sector-specific expertise and unfulfilled local demand to develop unique, world-leading cloud and edge services	11
1.1.2. Weaknesses and threats.....	13
1.1.2.1. European cloud offerings lack the end-to-end integration and one-stop-shop access to ecosystems sought after by customers	13
1.1.2.2. The cloud market is capital intensive, but market fragmentation and regulation hinder European firms' ability to invest and scale	14
1.1.2.3. Hyperscalers are picking speed in the race to own the future cloud-edge computing value chain.....	14
1.2. Our vision of the European cloud & edge technology landscape: 2025 and beyond	15
2. How can European industry bridge the gap?.....	18
2.1. Technology priorities for strategic investment by 2025.....	18
2.1.1. CLIMATE NEUTRALITY AND RESOURCE EFFICIENCY	20
2.1.1.1. Low carbon digital infrastructures (including AI / cooling / waste recovery technologies and blockchain certified recycling / green supply chain).	21
2.1.1.2. Disruptive technologies to enable zero carbon cloud & edge data storage & management.....	22
2.1.1.3. Cross-industry decarbonization data platforms.....	22
2.1.2. CYBERSECURITY	25
2.1.2.1. Zero trust identity management solution powered by AI.....	25
2.1.2.2. Innovative data encryption technologies including quantum safe encryption	26
2.1.2.3. Automated Security Operation Centres (SOC) for faster detection and response to cyberattacks.....	26
2.1.2.4. Edge cybersecurity (Secure Access Service Edge), for trusted architecture and network in collaborative edge	27
2.1.3. INTEROPERABILITY AND MULTI-PROVIDER SERVICES	29
2.1.3.1. European cloud services standards	29
2.1.3.2. Multi-Provider and Cloud-Edge Control-Plane (MPCP) and API Framework.....	30
2.1.3.3. Federated European cloud marketplace	32

2.1.3.4. Reference implementation for cloud and edge deployment – European cloud show case.....	34
2.1.4. NEXT GENERATION DATA CENTRE INFRASTRUCTURE	36
2.1.4.1. Increased density of central-cloud and edge facilities.....	37
2.1.4.2. Retrofitting of data centre facilities for improved energy efficiency and performance	41
2.1.4.3. Advanced data centre infrastructure management	42
2.1.5. NETWORK INTEGRATION AND INTERCONNECTIVITY.....	43
2.1.5.1. Network service technology to ensure performance at the Edge.....	45
2.1.5.2. Interconnectivity for European cloud and edge services	46
2.1.5.3. E2E service orchestration and assurance across network and cloud	47
2.1.6. NEXT GENERATION CLOUD-EDGE FOUNDATION INFRASTRUCTURE.....	48
2.1.6.1. Cloud infrastructure control plane.....	49
2.1.6.2. Cloud and Edge hardware design, integration and deployment	50
2.1.6.3. Hardware accelerated cloud native software for computationally intensive tasks on edge nodes.....	52
2.1.6.4. Edge-cloud native multi-tenancy	52
2.1.6.5. Edge hardware / software disaggregation	53
2.1.7. INFRASTRUCTURE SERVICES.....	55
2.1.7.1. Development of open standard/open source cloud software stack.....	55
2.1.7.2. First deployments of advanced IaaS/PaaS services.....	56
2.1.7.3. European “Telecom Cloud” reference implementation	57
2.1.8. PLATFORM SERVICES	60
2.1.8.1. End-to-end data pipelines and platforms.....	61
2.1.8.2. Middleware and Runtime capabilities enable large ecosystems	62
2.1.8.3. Managed Databases and custom operating systems for industrialization	63
2.1.9. APPLICATION & DATA SERVICES	66
2.1.9.1. Pan-European data sharing platforms	66
2.1.9.2. Application services enabling development of edge use cases	68
2.2. Enablers of success.....	71
2.2.1. Synergies with existing private and public initiatives, notably GAIA-X.....	71
2.2.2. Programs that align with digital sovereignty objectives should be supported or reinforced by the European Union and Member States.....	71
2.2.3. Regulation that enables the growth of European cloud and edge industry.....	71
3. Overview of technology priorities (2021-2025)	73
Example of roadmap and service dependencies for deployment (2021-2025)	74
4. A vision for European cloud-edge in 2030	75

Executive Summary

From cost savings and faster time-to-market to ground-breaking data and AI-based services across industry value chains, cloud-edge technologies foster a tremendous economic potential for citizens, businesses and public administrations.

Europe is no stranger to these technologies. The European Commission unveiled its first cloud computing strategy in 2012¹. To date, 36% of the continent's companies use cloud services², for an estimated €54 billion of direct cloud spending in 2020 – and that number is expected to double by 2023³.

Yet, the cloud and edge landscape has significantly evolved in recent years, and raises new challenges. Baseline technologies have matured, and client expectations have heightened. Most importantly the question is no longer centred on the value of adopting cloud computing, but on how to ensure supply meets heightened user demands in terms of openness, security, privacy and resilience, but also energy and resource-efficiency, and on how to best leverage the cloud-edge continuum to address sector-specific requirements.

Users – from industry and public sector to private citizens – wish to benefit from the diversity of services and performance standards that have been set by leading global cloud providers, while keeping ownership and flexibility over what they do in the cloud, as well as how their data is handled. They also wish to leverage cloud-edge technologies to increase their competitiveness, accelerate innovation and enable industry-specific needs. As digital technology invites itself into 'real-world' activities – from industrial production lines to autonomous vehicles and home entertainment – data is increasingly being generated and consumed 'locally', driving demand for data processing capabilities at the edge.

To date, the European market has struggled to match demand and provide a reliable alternative to global competition. It currently features a fragmented offering of solutions that are independently innovative, but that struggle to meet users' needs in terms of end-to-end coverage and ability to scale for the massive transformations due to place cloud and edge computing at the core of European business strategy and operations. One of the consequences today is that data from European firms contributes to train the algorithms and AI sold by non-EU based firms, increasing the existing technological gap. Europe needs to revert this trend.

As the backbone of the current and future digital economy, cloud and edge computing are also set to play an important role in achieving the bloc's collective ambition to reduce greenhouse gas emissions by 55% by 2030⁴ and achieve climate neutrality. The market will increasingly look for energy efficient cloud infrastructure and services. Born in pursuit of greater efficiency and optimal use of over-capacity, cloud computing can play a leading role in fighting climate change by integrating environmental considerations into its equation. Deployments "at the edge" can contribute to reduce data traffic and their carbon footprint.

To build the next generation cloud and edge offering, Europe must not look in the rear-view mirror and recreate what exists with a local flavour. The European market must invent what's next, focusing its energy in achieving a leapfrog in technology and competitiveness. Such leapfrogging will primarily stem from innovations that push the technological boundaries, especially in terms of ability to manage cloud-edge and multi-cloud environments, curb environmental impacts, and meet industry-specific needs, but will also involve standardisation – if not commoditisation – where technology is already mature.

Co-authored by representatives of 27 leading European industry players, the report provides a collective view of the technology domains requiring strategic investment to

¹ <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF>

² https://ec.europa.eu/eurostat/statistics-explained/index.php/Cloud_computing_-_statistics_on_the_use_by_enterprises

³ <https://www.statista.com/outlook/tmo/public-cloud/europe>

⁴ <https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030>

enable the development and adoption of competitive, secure, trusted, and climate-neutral cloud and edge services across the EU.

Priority investments revolve around three pillars:

1. **Becoming the leader in domains that will shape and showcase European cloud and edge offerings on the global market.**

By 2025, the European cloud-edge industry should be globally renowned for its technological leadership and competitiveness in terms of climate-neutrality, cybersecurity, trustworthy data exchange and interoperability, shaping worldwide standards. By developing high energy efficiency infrastructures, leveraging low consumption hardware and software, improving resource management, and enhancing data centre energetic mix & cooling performances, the EU could lead the way in developing sustainable cloud and edge offerings. In addition to eco-responsibility, security is a transversal and critical enabler of trust. Cutting-edge security across the spectrum of cloud-edge services and infrastructure, from edge devices to innovative hardware encryption technologies, will be a priority to secure adoption of European offerings. Technologies enabling secure communication networks as well as adequate management of access and cyberattacks are equally key. Furthermore, championing openness, interoperability and the ability to manage multi-provider ecosystem will help address the core of future market demand, empowering users to further adapt cloud-edge services to their own context. By defining shared standards and building central components that allow users to choose and assemble the best of what the market has to offer, European players can play a leading role in maximising the benefits of cloud and edge technologies to customers' competitiveness, growth and innovation.

2. **Renewing and expanding infrastructure foundations across Europe**

Increased density of edge and cloud facilities is needed to sustain adoption of innovative and sovereign edge and cloud technologies across the continent. Backed by ubiquitous connectivity to deliver the right performance in terms of bandwidth and latency, Europe's infrastructure will require advanced network management and orchestration technology as well as neutral interconnection services to guarantee efficient infrastructure utilisation, and enable innovative use cases at scale. The European market must also adopt cloud native 5G and enable industrial local 5G networks, leveraging the global competitiveness of its network equipment providers and the worldwide footprint of its telecommunication operators to transform the mobile network into a global network of widely distributed cloud-edge nodes.

3. **Enabling sovereign and sector-specific services to end-users**

Existing infrastructure service offerings must be strengthened, with a focus on providing businesses with sovereign options that match global standards in terms of price and resilience. European offers of platform services are still in their infancy and must be developed and deployed at large scale to allow the continent's industries to create high-added value services for the local and global market and accelerate the creation of use cases. Finally, this target cloud and edge offer should provide an open ecosystem of applications and toolkits, that foster innovation for the whole European ecosystem. Pan-European data sharing could only be enabled by dedicated European platform solutions and data exchange standards that provide the necessary trust and transparency to data owners, opening possibilities for unprecedented benefits for EU citizens, businesses and public administrations.

By building the next generation offering, Europe has the opportunity to own its cloud-edge transformation and set up success for its "digital decade" on the global stage. Existing public and private initiatives, notably GAIA-X, should be leveraged to align towards this common goal.

NB : as a technology roadmap, the report's recommendations are focused on investments and collaboration needed in terms of technology: this does not mean that the regulatory environment should not be considered reading the following document, and short section has been added for this purpose at the end of the report.

Glossary

API: application programming interface

BMC: Baseboard management Controller

CaaS: Containers as a Service

CPU: Central Processing Unit

FS: File System

GPU: Graphics Processing Unit

HPC: High-Performance Computing

HW: Hardware

IaaS: Infrastructure as a Service

IoT: Internet of things

NIC: Network Interface Card

OS: Operations System

PaaS: Platform as a Service

SaaS : Software as a service

SME: small and medium-sized enterprises

SSD: Solid State Disk

Introduction

The global cloud market is at a turning point: while traditional cloud services trend towards commoditization, innovation is progressively enabling a shift towards a fully-fledged central-cloud to edge-cloud continuum⁵. At the same time, demand is rising across the EU market for solutions offering greater openness, trust and control over data, and the cloud industry is increasingly coming under pressure to contribute to the environmental sustainability of the entire economy.

This document aims to provide the view of European industry on technology domains requiring strategic investment to enable the development and adoption of competitive, trusted, and sustainable cloud and edge services across the EU, building on existing strengths and future business opportunities. While cloud and edge services will intrinsically enable and benefit from other technologies (e.g. 5G, artificial intelligence, quantum computing...) to flourish, these domains are not specifically covered by the report's recommendations. Wherever possible, synergies with existing public and private sector initiatives should be leveraged – to take an example, the GAIA-X project has already taken steps to align on common frameworks for federated cloud services.

The document is structured in three parts. Section 1 provides an overview of the current EU market's strengths and weaknesses and gives a view of the ambition that the authors consider achievable by 2025, and beyond. Section 2 details the cloud and edge technology priorities for strategic investment, as well as several 'enablers of success' that European industry considers key to shift the paradigm towards that ambition. Section 3 presents a consolidated table and roadmap view of these priorities and maps the interdependencies between domains. Section 4 presents a vision of the technologies that could shape European competitiveness in cloud and edge computing beyond 2025.

⁵ This is henceforth referred to as the 'cloud-edge continuum' for simplicity.

1.Context

1.1. Where are we now?

1.1.1. Strengths & opportunities

1.1.1.1. A dense and technologically diverse ICT industrial base

Europe features a diverse ecosystem of cloud and edge equipment and software vendors, as well as a wide range of network infrastructure and data centre providers capable of hosting cloud services.

The distribution and density of office locations, data centres, on premise solutions, and network infrastructure across the European territory offers a level of customer proximity and intimacy that can provide a time-to-market advantage relative to hyperscale cloud providers.

The telecom network with its widely distributed architecture, and evolution towards cloud edge, poses a unique opportunity to leverage both the strength of European telecom vendors, who are globally leading in providing cloud native 5G⁶, but also the global footprint of European telecom operators.

The market equally benefits from established system integrators with the variety of skills to leverage this diverse infrastructure, and implement solutions tailored to industry needs, as well as a growing ecosystem of small cloud providers with strong infrastructure-as-a-service offerings.

European technology players are also well positioned in the field of data processing⁷, especially energy efficient super/hypercomputing, and have made leading contributions to research quantum computing that can be leveraged to develop world-class offers⁸. Moreover, while supply has primarily been driven by hyperscalers, the continent has also built ultra-low latency and large bandwidth networks to interconnect modern data centres and the industrial infrastructure. The expertise built in developing these networks and interconnectivity technologies offers a springboard to interconnect future providers, especially in the context of cloud federation. The continent also harbours a growing field of players in the cybersecurity sector⁹.

Finally, private investments have made European data centres globally competitive from an energy-efficiency point of view.

⁶Ericsson has been globally first with commercial 5G live networks in 4 continents, with 83 now live, and a total of 136 unique operators commercial agreements or contracts, <https://www.ericsson.com/en/5g#live-5g-networks>, Ericsson portfolio includes over 57.000 patents. Nokia's customers' radio networks support 6.6 billion subscribers worldwide (end of 2020). Nokia has 153 commercial 5G deals with service providers and enterprise customers, with 63 live networks. Nokia is in #1 position for granted 5G essential patents, with over 3500 patent families. <https://www.nokia.com/networks/5g/5g-contracts/>

⁷30 out the top 100 HPC / supercomputers worldwide are in Europe, and Europe features in the top 3 worldwide players (Atos).

⁸See EuropeQCI project (<https://ec.europa.eu/digital-single-market/en/news/future-quantum-eu-countries-plan-ultra-secure-communication-network>), for the development and integration of state-of-the-art and competitive European cybersecurity and quantum technologies. Other examples of European research in Quantum Computing and Quantum Communications: - Quantum Technologies Flagship (<https://ec.europa.eu/digital-single-market/en/quantum-technologies-flagship>) a number of basic research projects: CiviQ, QIA, Q-RANGE, UNIQORN.

- Also part of Horizon 2020: OpenQKD (<https://openqkd.eu/>), a demonstrator of Quantum Communications.

⁹To only name a few, recognized firms include: Stormshield, Tehtris, DataDog, Sentryo, Alsid. Like in many sectors however, several of these firms have chosen to list or sell their assets to non-EU firms and funds in order to scale.

1.1.1.2. Globally recognized standards and open innovation culture

The European market benefits from a dynamic open-source community¹⁰, which enables both transparency and innovation. This provides a fertile environment for further technological development, as illustrated through the increasing number of innovative SMEs and the multiplication of start-up hubs within the EU.

The EU has also distinguished itself as a norm maker in the technology field, contributing to the telecom evolution from 2G to 5G, as well as providing a legal framework for such things as quality understanding, process know-how, and strong regulation to protect data privacy and security. The European Union can utilize this capacity to ensure a more transparent, secure, and interoperable global market for cloud and edge technology.

Beside communication standards, European players are also playing a role in the standardisation of interfaces between information technology and operational technology solutions (IT/OT), to enable exchange of data for industrial applications. One example is the German Industrie 4.0 initiative which seeks to introduce a digital twin standard – named Asset Administration Shell (AAS) – for all manufacturing industries¹¹. The Industrial Digital Twin Association (IDTA) has recently been founded to enable manufacturing companies especially SMEs to adapt this digital twin approach.

1.1.1.3. Opportunities to leverage sector-specific expertise and unfulfilled local demand to develop unique, world-leading cloud and edge services

Europe has vibrant domain specific industry segments to build on. Furthermore, despite a relatively technologically advanced industrial base, cloud and edge penetration remains unevenly distributed, implying significant growth potential for these technologies. Across the EU, latest figures indicated that 36% of companies currently use cloud services – 21% for more advanced services – versus more than 50% of firms in the US¹². Moreover, the existing cloud offering does not sufficiently meet European industry demand for interoperability, energy and resource efficiency, and sovereignty.

Europe can utilize its leading and often unique domain know-how in certain high-growth industries to advance its cloud and edge ambitions. This is true for example for the retail, automotive, manufacturing, engineering, electronics, and chemicals sectors, as well as gaming. The domain know-how carries a unique competitive advantage to speed up development of the technologies and innovations that will underpin tomorrow's businesses and help innovative European companies to grow into world-leading companies.

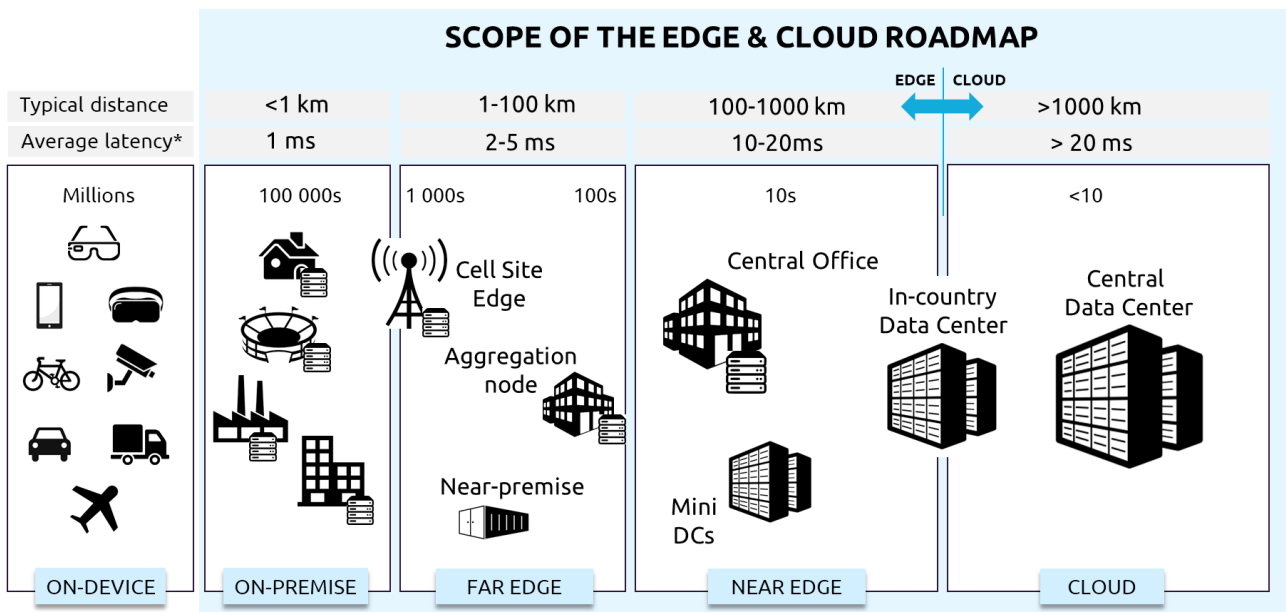
The European economy also holds significant untapped growth potential in cloud and edge services in sectors where penetration is low, such as manufacturing, transportation or aerospace-defence. Such industries face an economic imperative to adopt these new solutions and technologies, yet today only hyperscalers provide integrated offers for these services. As a result, many European firms still limit their adoption of such services, hampering their long-term competitiveness. The battle for these markets remains open, but the window for opportunity will be short, and whoever develops solutions that fit the sector needs will gain sector-specific expertise that can be leveraged internationally.

¹⁰ Including both EU-based foundations such as Eclipse Foundation, FiWARE, IDSA, and O4B but also global entities like Linux, Apache, or the Opengroup.

See also the EC communication on open source software strategy 2020-23 "Think Open": https://ec.europa.eu/info/sites/info/files/en_ec_open_source_strategy_2020-2023.pdf

¹¹ This approach is designed for the whole life cycle based on the reference architecture model RAMI 4.0 and incorporates also modern interoperability standards like OPC-UA and ECLASS.

¹² For Europe: https://ec.europa.eu/eurostat/statistics-explained/index.php/Cloud_computing_statistics_on_the_use_by_enterprises#Use_of_cloud_computing_highlights



* Latency does not depend only on distance. Other factors influencing latency are a) access technology (latency in 5G or FTTH much lower than in 4G), b) transport topology and technology, c) core network configuration (user plane location, breakout point), d) network optimization (traffic prioritization, bandwidth allocation, Edge node selection).

Figure: *Scope of the Industrial Roadmap in the cloud-edge continuum*

The European market also shows strong potential for growth in the use of edge technology, ranging from on-premise edge to “far edge” (i.e., at high proximity to customers and premises, within a range of 100km) and “near edge” (typically some hundreds of kilometres far from the customer), or even to regional data centres, due to its relatively low penetration to date, and strong business potential. The European economy could lead the deployment of edge technology by leveraging synergies with ongoing fibre and 5G rollouts as well as local presence of telecommunication operators and data centres. Telecom operators can also serve as vectors of penetration for new technologies.

1.1.2. Weaknesses and threats

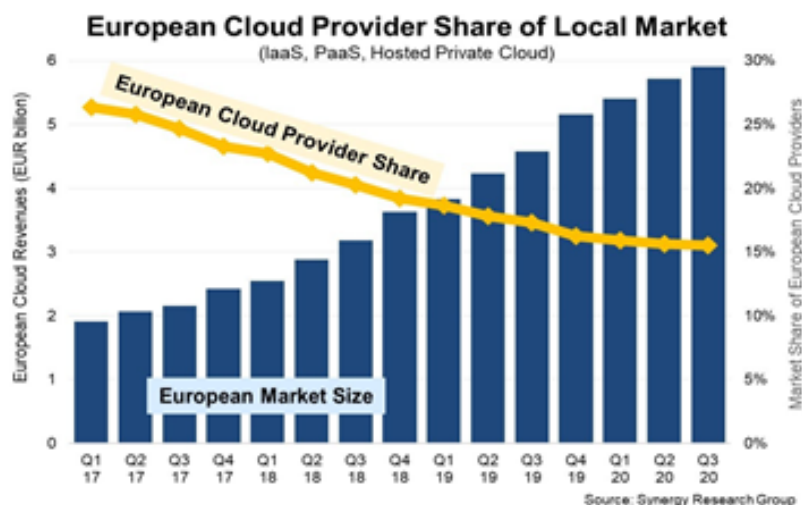


Figure: European Cloud Provider Share

European cloud providers have been losing market share compared to the main US cloud providers: from 26% in Q1 '17 to just 16% in Q3 '20, a loss of 10 points in less than four years¹³. This happened while the European cloud market grew more than threefold in the same period. Why are EU-based players struggling to capitalise on growth at home?

1.1.2.1. European cloud offerings lack the end-to-end integration and one-stop-shop access to ecosystems sought after by customers

While taken as a whole, European cloud offerings cover a wide spectrum of services, in practice, customers must work with many providers to achieve the quality and breadth of services provided leading global cloud providers. End-users seek simplicity and efficiency, and have become accustomed to 'one-stop-shop' offers that provide access to a suite of best-in-class cloud functionalities and tools they require – from IaaS to SaaS – and on a global scale.

Leading global cloud companies offer this integrated service thanks to standardization of their offers, as well as to the strong links they have built with a critical mass of provider ecosystems, distributors but also developer ecosystems, particularly through certifications.

European companies need to achieve scale and provide better functionality – including in areas like cybersecurity - to incentivize users to switch from existing, highly performant, non-EU providers to European alternative. Yet, the proprietary nature of this standardization and, the global critical mass makes it difficult for new players to emerge, particularly in the central cloud market where economies of scale and lock-in effects are strongest¹⁴.

¹³ <https://www.srgresearch.com/articles/european-cloud-providers-struggle-reverse-market-share-losses>. This also contributes to a downward spiral in revenue captured by European players, therefore less taxable income, further reducing the pools available for public investments into R&D.

¹⁴ Once a company or a Public Administration has a large amount of data within one Cloud provider, it is very difficult and costly, both in technical and economic terms, to move that data to another provider. When building a new product, it is relatively easy to adopt the latest innovative cloud solution. But migrating an existing data and business logic to a new cloud solution remains technically and financially challenging.

1.1.2.2. The cloud market is capital intensive, but market fragmentation and regulation hinder European firms' ability to invest and scale

Despite significant initiatives at European level to harmonize regulatory standards¹⁵, the continent's digital market remains fragmented into local realms, individually lacking the critical mass for players to scale and compete with their American and Chinese counterparts. Given the capital-intensive nature of cloud and edge services, particularly at infrastructure level¹⁶, these factors limit the emergence of globally competitive, innovative 'hyperscale' offers in Europe.

Taking examples from the telecommunications industry, fragmentation and barriers to long-term investment in infrastructure and new technologies result from:

- the setup of 5G spectrum allocation across EU countries, characterized by significant uncertainty as well as high spectrum prices that deprive candidate firms of the incentives and resources to invest in technology on par with their foreign competitors,
- a regulatory paradigm focused on achieving significantly lower consumer prices than in North American and Asian markets, undercutting European telecommunication operators' investment capabilities,
- regulatory regimes such as the ePrivacy framework that disproportionately affect legacy sectors, such as telecommunication operators, relative to online platforms

The current situation drives the return on invested capital (ROIC) for European service providers below the weighted average cost of capital (WACC), essentially removing their ability to invest in new infrastructure and technologies.¹⁷

Moreover, European providers and business consumers could engage more actively in the development of edge and cloud technologies. Cooperation between providers in the face of fierce global competition is lacking, and accentuated by insecurities regarding compliance of data sharing and pooling arrangements with EU competition law – something that the EU Commission aims to tackle by providing more EU guidance through its horizontal cooperation guidelines.

1.1.2.3. Hyperscalers are picking speed in the race to own the future cloud-edge computing value chain

Finally, the absence of European players capable of competing with global cloud players on software and hardware competencies, such as artificial intelligence, machine learning and silicon technology¹⁸, is accelerating the penetration of these firms into a breadth of European industries, from retail markets to automotive. With the experience of highly scalable cloud solutions, global players are pushing into the production facilities of the European industry with end-to-end solutions that further increase customer dependency. These initiatives will accentuate their strong market positions. The clock is ticking for investments that enable European industry to fulfil this demand competitively and regain a stronger position in the next generation of the cloud to the edge, which is still an uncharted territory.

¹⁵ Notable examples include the GDPR and the Free Flow of Non-Personal Data Regulation

¹⁶ The annual capital expenditure of the three largest US cloud companies – AWS, Azure, and exceeds \$60Billion per year.

¹⁷ The per capita investment in ICT infrastructure in Europe is 15% lower than in South Korea and more than half that in Japan and the USA. Overall, the European Investment Bank estimates the total investment required to meet Europe's 2025 connectivity targets is €384 bn of which only €130 bn will come from private investment.

¹⁸ Example: Nvidia with GPUs, Google with TPUs

1.2. Our vision of the European cloud & edge technology landscape: 2025 and beyond

Our aim is that by 2025, European industry stands as the leader in terms of energy-efficiency, cloud security and openness of cloud services notably including interoperability. To meet European – and global – customer demand for integrated and trustworthy solutions, services will need to be interconnected, easy to consume, and built on common standards and values that build trust in data management and data exchange: security, data protection, transparency and sovereignty. This cloud market would be built as a strong distributed cloud federation which is competitive in functionality, scale, performance and price, provides the foundation for sovereign digital services and enables the transition towards carbon neutrality of the continent's digital activities.

The current cloud market provides high levels of functionality at the cost of openness. The best of both worlds is to provide for an open yet integrated ecosystem of solutions. This approach - a core value proposition of GAIA-X – is a core principle of the technology investment priorities outlined in section 2.1, most notably domain 3 focused on ensuring interoperability across providers of the future European cloud offering.

Europe must promote open innovation and industrialize the cloud-edge value chain

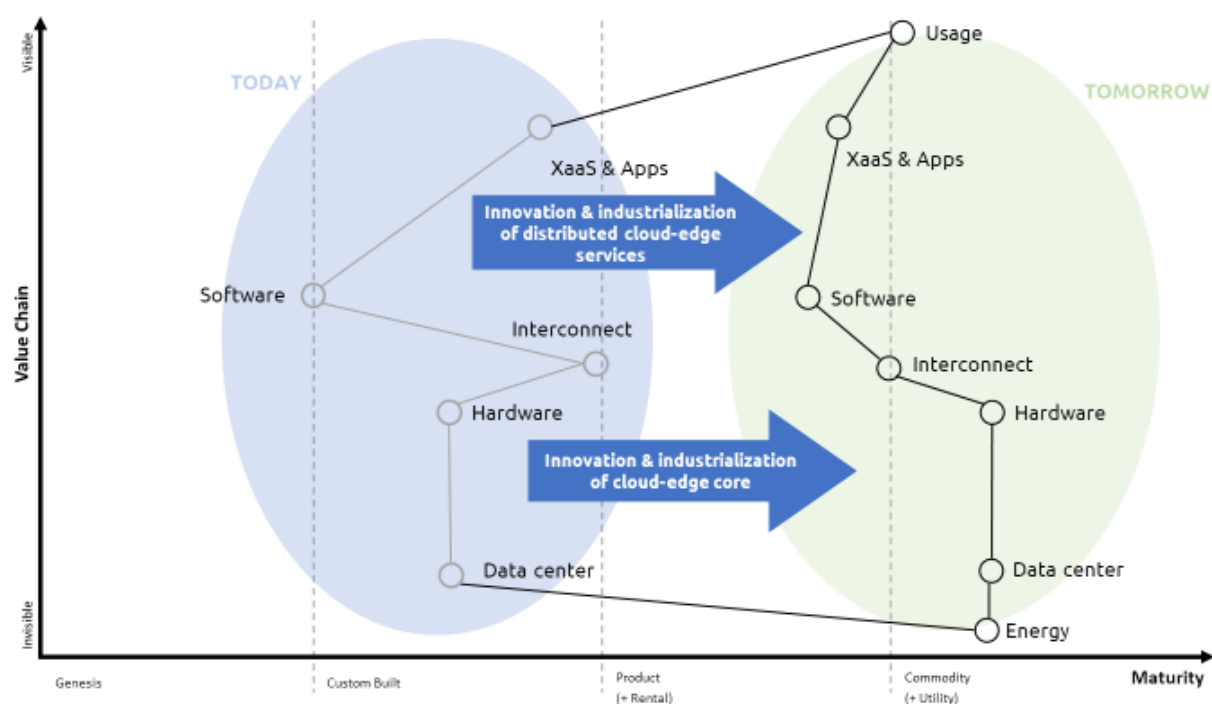


Figure: While global market leaders have built their market share by driving existing offers towards custom, proprietary standards, this roadmap aims to industrialize the cloud-edge core and enable greater innovation and competition of distributed cloud-edge services

The investment roadmap aligns with EU targets to double the use of advanced cloud services by 2025¹⁹ and raise it 75% by 2030 and achieve climate neutrality of data centres across the

¹⁹ Compared to 2018 levels <https://eur-lex.europa.eu/legal-content/en/TXT/?qid=1600708827568&uri=CELEX:52020DC0575>

EU by 2030²⁰. In doing so, the roadmap also aims to achieve the EC's *Digital Decade* target of deploying "10,000 climate-neutral and secure edge nodes" across the EU, open and distributed in a way that will guarantee access to data services with low latency wherever businesses are located.

The present roadmap also aims to achieve European software and operational sovereignty (defined below) by 2025 and launch initiatives towards reaching hardware sovereignty by 2030.

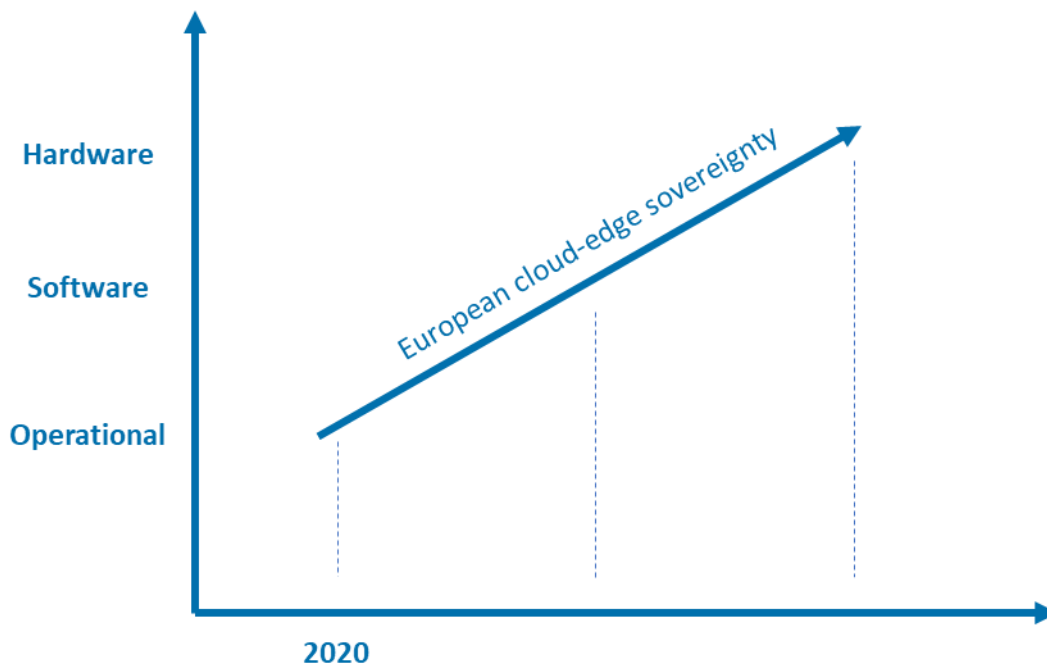


Figure: European next generation cloud-edge sovereignty ambition

Operational sovereignty: The capability to operate a cloud based on required scalability, reliability and cost. Infrastructure and software technology supply remains dependent on non-European players.

Software sovereignty: Operations and software supply can be sourced from European players and/or on an open-source basis. Hardware is still partly provided non-European players.

Hardware sovereignty: Operations, software and hardware technology can be sourced from European players and/or on European-registered open-source basis.

NB: Control implies choice – i.e. self-determination. It does not mean that all the continent's software and/or hardware is built in Europe, but rather that European firms and public institutions have the ability to find suppliers that answer their needs, and the economic, legal and operational ability to verify that those needs are indeed met. This could imply the existence of European-made – or European-owned – solutions where the market requires it.

To achieve the goal of a competitive distributed European cloud, highly efficient infrastructure is the necessary foundation for successful cloud services on top, like infrastructure services (IaaS), platform services (PaaS), and software services (SaaS). Highly efficient use, utilization and operation represent key success criterion for cloud platforms.

²⁰https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_en_4.pdf
Digital Decade 2030 targets: https://ec.europa.eu/info/sites/info/files/communication-digital-compass-2030_en.pdf

Through a high level of standardization and hyper-effective proprietary tools, hyperscale cloud providers generate an efficiency advantage up to five times that of today's standard enterprise data centres²¹.

The picture below shows the complication of the current central vs edge cost structure. Since Europe is aiming for a more distributed environment, target cost for edge services must be reduced to be competitive. New optimized edge hardware and management concepts are required, to provide competitive edge services.

Standardization and cooperation will reinforce Europe's leadership potential by enabling the emergence of federated services that combine subsets of the continent's edge and cloud infrastructure. This should include a durable relationship between public cloud providers, telecommunications companies and end-users capable of guaranteeing a new ecosystem both in terms of services and the underlying architecture. European collaborative edge platforms could also be developed further, based on open standards and maximized use of open-source code to reinforce competitiveness, portability and interoperability.

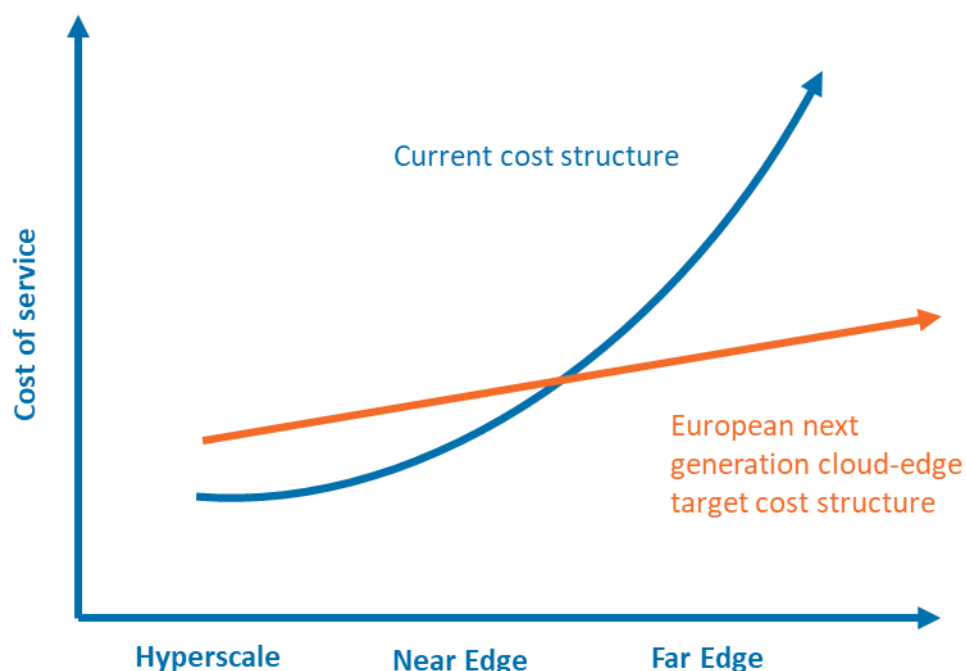


Figure: Cloud-Edge cost of service

²¹ Google is claiming to run an admin to server ratio of 1:10000 compare to 1:50/100 for average enterprises. Via 451 research report AWS data centres are 3.6x more energy efficient than standard on premise data centre and proceed the same task with 88% lower carbon footprint. <https://d39w7f4ix9f5s9.cloudfront.net/e3/79/42bf75c94c279c67d777f002051f/carbon-reduction-opportunity-of-moving-to-aws.pdf>

Gartner estimated that Google already ran 2,5 million servers in 2016. Public information puts European cloud provider operations at circa 300K server today. Considering a 50% growth of Google result in a ratio up to 1:40.

2. How can European industry bridge the gap?

2.1. Technology priorities for strategic investment by 2025

Addressing and achieving these collective ambitions can bring European private and public players together in overcoming a step change in innovation, through joint investment.

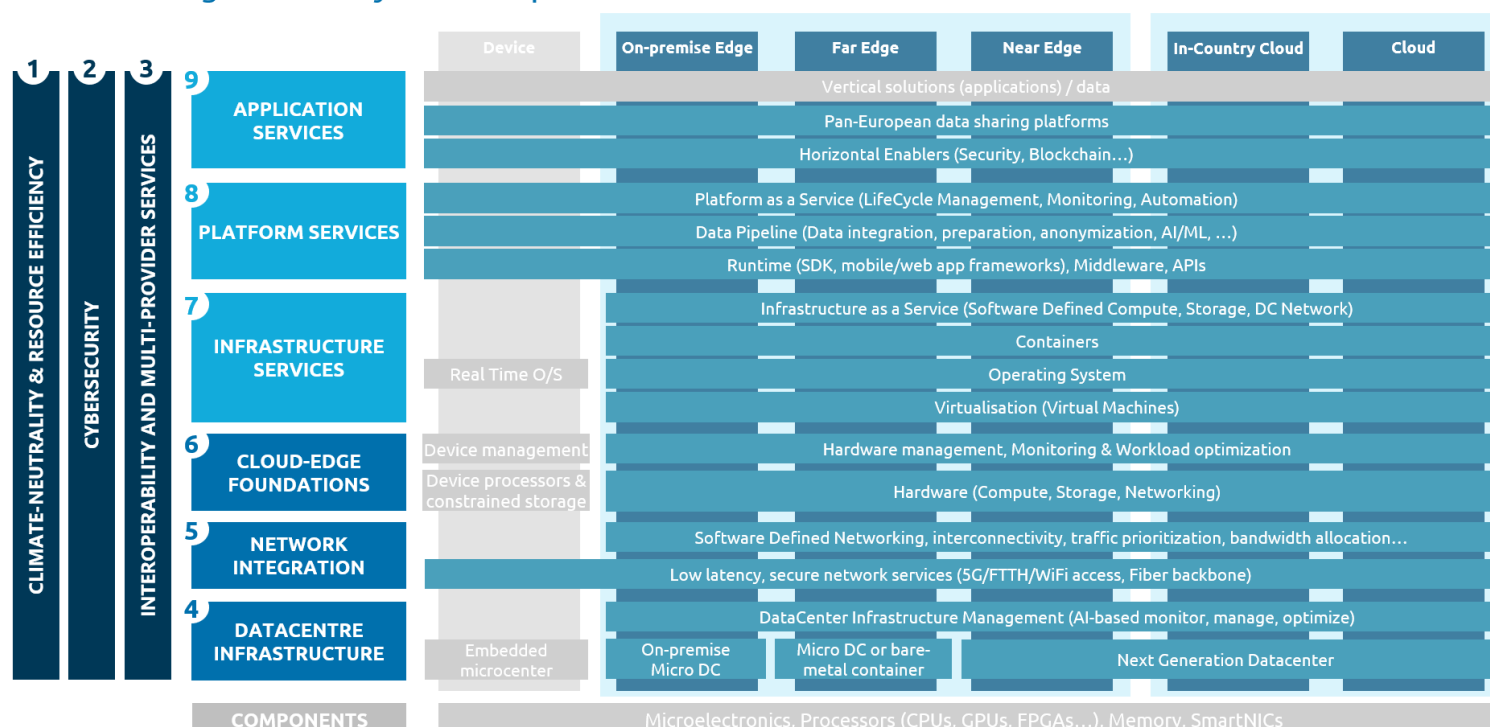
The following section outlines 30 technology priorities, falling into three broad categories:

- Investment domains 1-2-3 cut across the cloud stack to optimize end-to-end energy consumption, environmental impact, cybersecurity and the ability to choose and switch between providers
- Investment domains 4-5-6 serve to develop the necessary infrastructure (from network and data centre to cloud hardware & software) to enable harmonized and easy access to cloud services across Europe
- Investment domains 7-8-9 leverage these capacities to provide best-in-class, open and interoperable cloud-edge services to European public and private organisations and beyond.

A selection of **practical uses cases** featured throughout the document illustrate how these investments will enable real-world applications that transform industries across Europe, and even globally.

Technical scope of domains covered by the next generation cloud-edge industry roadmap

Out of scope of the Next Generation Cloud-Edge technology roadmap



Note on investment priorities and figures:

The investment needs for each priority have been estimated based on market studies, industry expertise and internal referentials – where possible these assumptions are provided in the text.

The roadmap only features technologies requiring a form of public investment – innovation and deployments that will be 100% funded by private sector are therefore omitted.

A rationale for public intervention, in the form of public investment, may result from the existence of market failures that hamper the market's ability to optimally respond to identified needs. When referenced as the rationale for public investment in a specific priority of this document, '**market failure**' indicates the absence of economic incentives for private sector players to optimally invest in the development of said technology over the provided period. Such inefficiencies are most often due to asymmetries in information, coordination and network failures, as well as insufficient consideration of externalities and public goods/knowledge spill-overs²². Beyond fulfilling market needs, technology investment may also be driven by policy imperatives and/or seek to improve 'public goods' (open-source contributions, achievement of sovereignty requirements...) which the market will not provide organically.

Other technology priorities, despite being lucrative at scale may still be too **capital intensive** relative to European industry's investment capacities in the short term. Some priorities will require investments to help European players pre-position and **pre-empt future demand** rather than leave the market to players that can afford more long-term investment strategies.

²² See notably paragraph 45 of *Commission Regulation (EU) No 651/2014 of 17 June 2014 declaring certain categories of aid compatible with the internal market in application of Articles 107 and 108 of the Treaty*: "...market failures may prevent the market from reaching optimal output and lead to inefficiencies related to externalities, public goods/knowledge spill-overs, imperfect and asymmetric information, and coordination and network failures."

2.1.1. CLIMATE NEUTRALITY AND RESOURCE EFFICIENCY

Digital services and infrastructure generate around 4% of the current global carbon emissions²³, and such proportion may further increase due to the exponential trend of data creation. Irrespective of the total consumption, the expansion of cloud in Europe will result in significant energy efficiency gains compared to other alternatives, like on-premise or private clouds. Furthermore, an optimal allocation of activities between central and edge capacities will bring additional benefits, by optimizing network data traffic.

While central cloud solutions benefit from greater economies of scale, the distributed nature of edge cloud infrastructure will enable a smarter distribution of data across the network. Data which is used more frequently can be stored closer to the customer at the edge of the network while less critical data, which is retrieved less frequently, can be located further away in the network. This distributed architecture can generate new efficiencies and reduce the power consumption per data used.

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 digitalization of more traditional industry sectors such as manufacturing or logistics. Energy savings resulting from the use of cloud and ICT are many times higher than the ICT sector's own footprint (estimated 15 to 20%²⁴). 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.

Overall, a sizeable investment would allow to accelerate the integration of cloud and edge digital infrastructures in energy systems and to 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 efficiency technologies such as liquid cooling, the optimization of recycling in the supply chain, and the research in new technologies such as DNA storage, 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 priorities²⁵. The European Commission can support these efforts through the adoption of reliable sustainability criteria (KPIs) for data centres.

²³ [The carbon footprint of the digital sector \(europa.eu\)](https://ec.europa.eu/eurostat/tgm/table.do?tab=table&init=1&code=sdg_13_7_1&plugin=1)

²⁴ [Digital technology can cut global emissions by 15%. Here's how | World Economic Forum \(weforum.org\)](https://www.weforum.org/articles/digital-technology-can-cut-global-emissions-by-15-percent-here-s-how)

²⁵ [ClimateNeutralDataCentre.net](https://climatenutraldatacentre.net)

Edge to Cloud decarbonization

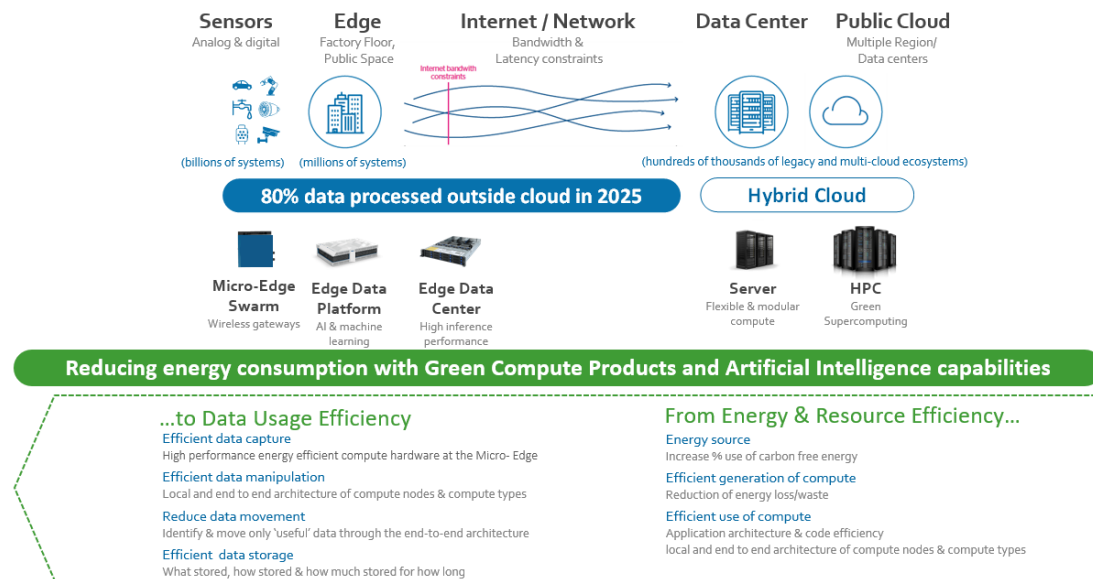


Figure: Edge to Cloud decarbonization

2.1.1.1. Low carbon digital infrastructures (including AI / cooling / waste recovery technologies and blockchain certified recycling / green supply chain).

The objective of carbon neutral cloud and edge infrastructures requires the implementation of advanced monitor and control systems to optimize energy and resource efficiency. They should be supported by technology investments in three directions, where European support could significantly accelerate the deployment pace versus current market trends.

- **Digital infrastructures should act as role models, opting for green energy sources.** Conversely, they should avoid creating climate and environmental damages by avoiding - in so far as possible - the recourse to fossil energy or excessive use of water. They should better integrate in energy systems by generating renewables on-site or strengthening grid stability by facilitating peak shaving. Green energy artificial intelligence should be developed to interface data centres and electricity grids, predicting and matching power consumption demand, especially when leveraging green hydrogen. The development of optical transmission infrastructure would also allow central data centre locations in cooler climate areas.
- **High energy efficiency digital infrastructures must be created.** They require the development of advanced technologies, such as direct liquid or immersive cooling, waste heat recycling, and High Performance Compute zones with in-rack-row cooling that includes adiabatic cooling technology (see section 2.1.4.2 for further developments). For the cloud applications, artificial intelligence tools must be developed to monitor ensure all application code is written with power efficiency in mind, refactoring to refresh applications to leverage cloud features for more sustainable operations.
- **Thorough Recycling** to maximize component lifecycle management by designing for longevity (infrastructure modularity, repairability, upgradability ...) and ensuring recycling when the reuse of components is no longer possible (avoid the practice of purposefully destroying well-functioning storage equipment. Blockchain technologies should be further standardized on energy efficient and light weight solutions. They should also be further developed to get an immutable record of green certified information on the cloud and edge supply chain (hardware).

More widely, Europe could leverage its leading position in hydrogen and green supply technology development to generate a global competitive advantage.

Required investment by 2025	200 M€
Rationale for investment	Capital expensive
Private:public ratio of expected investment	50:50
Is funding required to cover development, deployment, or both ?	R&D - <i>Investments for deployment are already covered in section 2.4.1</i>
Should investments be national or cross-border?	Cross-border

2.1.1.2. Disruptive technologies to enable zero carbon cloud & edge data storage & management.

The total amount of data in the world is currently estimated to be around 60 zetabyte²⁶ and is expected to continue growing at an exponential rate over the coming years, reaching beyond 160 zetabyte in 2025²⁷. This is unsustainable 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. Technologies such as DNA storage, which although may currently be an immature technology, could become the low carbon digital data storage medium of the near future. This should be complemented by a strategy that aims for a more efficient distribution of data within the networks, bringing mission-critical data closer to the customer. This would also acknowledge the limited technical possibilities infrastructure providers have to save energy in the light of exponential data growth.

Required investment by 2025	100 M€
Rationale for investment	Market demand
Private:public ratio of expected investment	50:50
Is funding required to cover development, deployment, or both?	Development
Should investments be national or cross-border?	Cross-border

2.1.1.3. Cross-industry decarbonization data platforms

The Cloud & Edge industry, as the rest of the industry, would benefit from cross-industry decarbonization data platforms and have a leading role to play in deploying them. These include the automated collection of data, the development of eco-efficiency metrics, the simulation and forecasting analytics and artificial intelligence capabilities. Such data platforms have not naturally emerged from the market at wide scale today since they require cross-company analysis and industry investments.

One can expect from such platforms cloud and edge resource optimization to provide clear real-time visibility of resource utilization and workload management. It would also enable predictability of resource scaling up and down, to ensuring optimal energy usage, better use

²⁶ <https://www.statista.com/statistics/871513/worldwide-data-created/>

²⁷ IDC Data Age 2025: <https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy#projected-figures-2025>

of on-demand-cloud-scalability, required investment in management solutions, load distribution, and automation. In addition, an effort of standardization is needed for the proper carbon emission data reporting to enable aggregation of data from multiple sources.

Europe could become a global leader in this domain if it succeeds in creating the necessary ecosystem of companies and technology partners to jointly develop these decarbonization dataspace and deploy the supporting data platforms. Ongoing initiatives like Gaia-X can help to achieve these goals.

Required investment by 2025	100 M€
Rationale for investment	Market failure
Private:public ratio of expected investment	30:70
Is funding required to cover development, deployment, or both?	Deployment
Should investments be national or cross-border?	Cross-border

USE CASE: AN AI ENABLED, ECO-FRIENDLY PLATFORM, TO SUPPORT COLLABORATION IN THE EU HEALTHCARE SYSTEM (MORE CARE, TO MORE PEOPLE, MORE EFFICIENTLY)

Overview

Highly fragmented healthcare systems and proliferation of Data Silos are part of the challenges today driving the current increase in Healthcare spending in Europe which represents 10% of EU GDP²⁸ and continues to exceed GDP growth. Healthcare emissions are equivalent to 4.4% of global net emissions. If it was a country, it would be fifth largest emitter.

The challenge

Digital is driving a Healthcare transformation that will enable the EU to provide better care at reduced costs all while improving the healthcare industry's carbon footprint, currently negatively impacted by legacy data centre infrastructure with duplication and transmission of large data sets. One specific dimension of this transformation is related to AI. Specifically, the use of "federated" data sources to build AI models securely and efficiently, while respecting EU data and privacy and regulatory initiatives/mandates. To achieve this goal, a few fundamental challenges need to be addressed:

- **Manage a data Ecosystem...** where the enabling data platform ensures secure access to - and compliant usage of - data. This requires efficient and effective controls across the entire data lifecycle. From the point of data capture through data manipulation, movement, and storage. These controls not only ensure data security and compliance of usage, but also optimize Data usage Efficiency (DuE) to reduce overall energy consumption in the Healthcare ecosystem that is sharing the data.
- **Build "federated" AI...** which requires the enabling platform to integrate and orchestrate where and how AI learning takes place across multiple edge locations. This enables the same AI algorithm to be "trained" on multiple data sets without having to move the data from the edge to a centralized cloud location. This not only addresses data security and compliance concerns but also reduces energy consumption as data volumes do not move from the edge to the cloud. The resulting "inference Machine Learning" model that is then shared across all the edge locations is more accurate due to the larger and more diverse type of data sets used.

The benefits that eco-friendly platform's AI Federation capabilities would provide to the EU Healthcare ecosystem include, but are not limited to:

- **Imaging Centers with AI driven diagnostics** (more effective models)
- **Remote Care** (more effective care) that improves Physicians' ability to advise patients remotely, providing automated recommendations based on actual data that is processed by ML algorithms that have been trained on not only data sets from patients under the Physician's control but also from data sets from citizens across the EU
- **Remote Care** (more types of care) that allows Physicians to work more efficiently through support from AI models. This would help them provide specialized care to patients who may not otherwise get it, especially in underserved populations.

From a decarbonization perspective, such benefits would have a significant net positive impact, the efficiency gains of precision medicine overwhelming by one order of magnitude the additional carbon footprint of increased AI and data processing.

To meet the Healthcare industries needs in this domain a holistic approach towards data, infrastructure and AI models is proposed. The foundation of the solution is a compute continuum (edge to cloud) combined with artificial intelligence designed, built, and run to optimize energy consumption while respecting SLA and data compliancy requirements. Key solution components are:

- **Efficient & Effective Compute**
High performance, highly efficient infrastructure supervised by AI should optimise multiple dimensions of energy consumption, relating to the infrastructure itself (cloud & edge, energy efficient computing power, waste heat recycling...). It should also optimise application architecture, code efficiency, the efficient data manipulation with local and end to end architecture of compute nodes and compute types and the reduction of data movement by identifying and moving only 'useful' data through the end-to-end architecture.
- **The AI Models**
Frugal AI, combined with high performance compute for effective AI model training in Edge locations, combined with explainable AI to meet compliancy regulations would optimize the decarbonization impact.

²⁸ Source: Eurostat by European Commission, March 31, 2020. <https://ec.europa.eu/eurostat/web/products-eurostat-news/-/DDN-20200331-1>

- **Optimised data storage**

Carbon efficiency would also benefit from the elimination of useless data volumes, the AI supervision to optimize storage methods of useful data as where and how long data to be stored

2.1.2. CYBERSECURITY

The overall cost of cybercrime to the global economy has doubled since 2015, reaching an estimated € 5.5 Trillion at the end of 2020. A recent poll of executives in Germany, France, UK, and US revealed that 90% of companies have faced increased cyberattacks during the Covid pandemic²⁹. It is therefore imperative that Europe takes a leading role in cloud and edge security to ensure trust and confidence in industrial data management. In particular, the adoption of modern applications and cloud native technologies which support the cloud – edge continuum requires new security paradigms and control.

As an illustration, data spaces require security at transit and secure interconnections between the different stakeholders. Secure interconnections can be provided by Internet and cloud exchange points, by separating the data traffic at network level, limiting the paths from data sources to destinations, and by introducing concepts such as Closed User Groups or applications to mitigate DDoS attacks, including in supply chain.

Taking such a leadership position in digital security will require major investments, in the range of 1.5 Bn€ over the next 4 years.

2.1.2.1. Zero trust identity management solution powered by AI

Europe must develop a reliable, high-performance, **zero-trust identity management solution** which 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, recertifications, reconciliations of rights over applications. The adoption of Trust and Auditing Distributed Ledger Technologies to enable certifiability for specific target surfaces in the cloud and edge infrastructure is required to support EU-strategic sector demands and to ensure dynamic software safety assessments. Such emerging technologies will contribute to technological sovereignty and require European public support for faster development and deployment.

Required investment by 2025	500 M€		
Rationale for investment	Pre-empt demand	future	market
Private:public ratio of expected investment	50:50		
Is funding required to cover development, deployment, or both?	Both		
Should investment be national or cross-border?	Cross-border		

²⁹<https://www.tanium.com/press-releases/tanium-report-reveals-90-percent-of-organizations-experienced-an-increase-in-cyberattacks-due-to-covid-19/>

2.1.2.2. Innovative data encryption technologies including quantum safe encryption

Europe should support the development of next generation cloud security solutions that provide a single panel of glass in security controls, in order to ensure security policy is consistently deployed across the heterogeneous cloud environments. Such solutions provide the layer of trust in hybrid cloud and multi-cloud environments. This allows organizations to maintain full control over the security and protection of their data in the cloud, the data transfer from on-premise or cloud infrastructures, as well as cyberprotection for AI applications and SaaS services. They include the advanced development of trusted encryption in industrial harsh environmental conditions (high vibration, temperature, pressure...).

They also encompass solutions giving the ability to maintain data in a continuous encrypted state so that to work on them without decrypting, such as homomorphic encryption. 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 and require European public support for faster development and deployment. Europe could become a global leader in these technologies by leveraging existing ecosystems of partners, intensive R&D activity and ongoing initiatives like Quantum Flagship.

Required investment by 2025	500 M€
Rationale for investment	Complex, high risk (and cost) research, Uncertain time-to-market (and uncertain timing at which demand will emerge, given it will depend on speed of progress in quantum computing)
Private:public ratio of expected investment	30:70
Is funding required to cover development, deployment, or both?	Both
Should investments be national or cross-border?	Cross-border

2.1.2.3. Automated Security Operation Centres (SOC) for faster detection and response to cyberattacks

The continuous trend towards a high volume of simultaneous or AI-based cyberattacks targeting critical digital infrastructures requires further integration of machine learning and AI assisted automation technologies in security operations to improve threat anticipation (access, data privacy, login, certification), detection (data analytics, tracing), and response (incident and problem management). Improvement of AI-based security analytics supported by automation in areas such as policy/compliance as well as forensic & incident response are also key to anticipate attacks or to mitigate them. Such technologies include deep learning for cybersecurity, such as algorithm for deep behavioural profiling and anomaly detection.

Required investment by 2025	250 M€
Rationale for investment	Market demand
Private:public ratio of expected investment	70:30
Is funding required to cover development, deployment, or both?	Mainly deployment
Should investment be national or cross-border?	National

2.1.2.4. Edge cybersecurity (Secure Access Service Edge), for trusted architecture and network in collaborative edge

Edge cybersecurity (Secure Access Service Edge) must be built to ensure a 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), data loss protection (DLP). Standard IAM (Identity Access Management) and SSO (Single-Sign-On) services developed for cloud computing environments will also require significant R&D to reach a comparable level of maturity and resilience in edge environments. Such emerging technologies are critical to ensure edge technological sovereignty and need to be bundled to edge investments.

Such Secure Access needs to become an integral part of 5G Mobile Networks offering software defined networking in WAN and Secure Access Service Edge functionality for Enterprise networking. This requires 5G to be tightly integrated with edge, networking and security functionality to an end-to-end network. It will also require availability and integration of end-to-end service orchestration of SD-WAN, SASE and Mobile Networks across the full solution.

Required investment by 2025	270 M€
Rationale for investment	Market demand
Private:public ratio of expected investment	50:50
Is funding required to cover development, deployment, or both?	Both
Should investments be national or cross-border?	Cross-border

USE CASE: SMART AND SECURE CLOUD AND EDGE FOR INDUSTRY 4.0

Overview:

The arrival of Internet of Things (IoT) blends physical and digital worlds with exponential growth of raw data from wide range of sensors in plants, employees, products and machinery. Changes that IoT, 5G, AI, Edge computing and other technological disruptions can bring to companies to manage physical assets and their customers will introduce radical disruption in manufacturing business models, both for large and medium size companies.

It is estimated that only 1 percent of data from manufacturing plants is used today, mostly for anomaly detection and control, not optimization and prediction, which would provide greater value. cloud and edge technologies are therefore a critical enabler of Industry 4.0, with many use cases improving the operations of the manufacturing organizations, such as predictive maintenance, precision control, Augmented Reality/Virtual Reality (AR/VR) in manufacturing plant, digital twins, cloud industrial supervision, 3D printing, robotics and cognitive automation, digital traceability, etc. In particular, edge computing will gain increasing importance as it allows data processing close to the manufacturing devices, reducing latency and allowing real-time prescriptive analytics. These digital solutions also need to integrate security by design to protect the manufacturers' data, intellectual property and the continuity of their operations.

Solutions:

- **Edge-specific infrastructure and hardware** – computing, storage and networking hardware capable of running efficiently on resource constrained devices. Edge compatible operational platforming services, more specifically capabilities related to edge infra / platform / service monitoring, QoS and bandwidth management, network self-healing or edge device health monitoring
- **Security at the edge** building Security algorithms that would be implemented in the Edge servers directly for advanced detection and inference as well as security algorithms across the multi-cloud & hybrid cloud environments.

- **Identity Management and advanced access control at the edge:** with AI-augmented identity and access management capabilities. These mechanisms will help security officers detect anomalous behaviours, insider threats, situations that are not compliant with Zero Trust principles
- **Zero Trust at the Edge:** organizations will be able to manage IoT Access control, enable advanced security controls depending on the criticality of the data, and secure all connectivity in their environments. Such solution would fulfil the IT-OT continuity principle for what concerns access control and control access from users to objects, objects to services as well as services to services, provide encryption solutions, trust assessments, DLP, Secure Gateway, Threat prevention, Data privacy etc.

2.1.3. INTEROPERABILITY AND MULTI-PROVIDER SERVICES

The creation of a common sovereign European cloud, with the participation of European companies, the European Union and Member States, would create a more uniform European cloud-edge landscape. These could consist of basic services that can be expanded and adapted by providers under the rules of comparability.

Common cloud refers to cloud infrastructure, platform 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). Distributed services must have a possibility for the user to manage them centrally and easily via a Service orchestrator. In a distributed system, services like interoperability, security and interconnection are of greater importance. In order to ensure variety of services, it must be possible to provide comparable services from several providers. Service access, compliance and quality must also be based on common standards with strong focus on user requirements and usability.

Based on Europe-wide defined or adequate international standards, the development of joint services and offers is necessary in order to guarantee a high degree of interoperability, portability and reversibility of infrastructure and data.

Digitalization needs interoperability – also supporting the possibility for 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 for different verticals are necessary and may be provided from different vendors. Interoperability – inside one vertical or cross vertical – is a must. Therefore, the creation of and compliance with binding European (and possibly international) standards is of central importance to the sustainability of solutions and thus is a competitive strength³⁰.

Preferably these standards should be global – because only global standards ultimately lead to success in a world that is more and more connected and where multinational companies make sizeable contributions to national GDPs. Ultimately, standardization must be done at best in international standardization committees, but European policy makers and industry must play a leading role in driving these standards in accordance with the continent's vision.

To enable portability, standardized and open APIs are crucial. Besides the specification of those open APIs, this also comprises the provisioning of open documentations and open reference implementations of client libraries for those open APIs.

Investment areas are all around interoperability, portability and reversibility to ensure the freedom of choice for management and workload distribution between new EU clouds/edge and existing cloud environments.

2.1.3.1. European cloud services standards

In order to provide consistent service within a European cloud ecosystem, significant standardization is required³¹. Aligned within the European values and market fairness, these standards need to be open and accessible without limitations regarding IP and licencing. Standards should cover, but not be limited to API, portfolio, quality, security and compliance.

³⁰ This technical approach to interoperability is a must have, but the regulatory request for interoperability is a must-have as well to ensure that "gatekeepers" do not hinder such access. Therefore, proper enforcement of the Art. 6 of the Free Flow of Non-Personal Data regulation, as well as the inclusion of interoperability request within the "Digital Market Act" regulatory proposal by EC are key enablers.

³¹ These standards should leverage the work initiated by initiatives like GAIA-X Policy rule and architecture of standard. https://www.data-infrastructure.eu/GAIA-X/Redaktion/EN/Publications/gaia-x-policy-rules-and-architecture-of-standards.pdf?__blob=publicationFile&v=5

The implementation of such open standards will enable a high level of interoperability, portability, reversibility and interconnectivity, as well as to provide service diversity. The standards should cover in the beginning a basic set of infrastructure services, such as compute, storage, network and cloud native services, like container and container management. They will then extend across the complete cloud-edge continuum. The establishment of an agile standardization body is necessary, to support innovation and fast implementation.

The investment intends to cover the definition of standards based on existing standardisation work and initial setup of a standardisation framework and governance. This work will not necessarily require the creation of new standardisation bodies, but rather the consolidation of such standardization for existing European Standardization Organizations³² to approve and promote them across the EU and globally.

Required investment by 2025	50 M€
Rationale for investment	Market failure, as this would be an international public good
Private:public ratio of expected investment	20:80
Is funding required to cover development, deployment, or both?	Development
Should investments be national or cross-border?	Cross border

2.1.3.2. Multi-Provider and Cloud-Edge Control-Plane (MPCP) and API Framework

Even if all their sovereignty needs may not be addressed, European companies already consume cloud services, often from various providers. Managing multiple providers, and their different services adequately, raises a challenge: how to handle the inherent complexity of bringing multiple providers together.

Despite the attractiveness and the quality of its services, proposing a European sovereign offer will add onto the complexity of managing multi-cloud environment as it will represent another provider to manage for the consumers, additional services to integrate. As European actors will not migrate all their workload to the sovereign cloud, it is key to anticipate this complexity, and to keep it as low as possible to ease the adoption of our solution.

The European cloud-edge offering should create and implement its core services (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. Building European cloud-edge offerings on the basis of Open Source components when possible, should be considered to favour appropriation and enforce security.

In addition to the “simplicity by design”, the European market should offer interoperability features and modules to ease its integration for end users and enforce its compatibility with other cloud providers solutions. It should offer an automated service discovery module, to scan networks and identify resources to ease their migration from one cloud to another. It should also offer transparent service and pricing discovering tools, to easily track used services, and their costs, to provide a clear overview of cloud usage across the different providers.

³² <https://www.cencenelec.eu/standards/ESOs/Pages/default.aspx>

But most importantly, it should provide the possibility to manage and deploy resources on different cloud environments, on different cloud providers. The MPCP should capitalize on standardized APIs and services to ensure their portability with existing cloud provider and offer north bound APIs and User Interfaces to manage DevOps and basic configurations. As a centric part of a multi-cloud environment, MPCP should be highly secured, with enforced data privacy mechanisms.

The investment should cover the initial development blueprint, if possible, based on existing Open-Source projects, as well as a reference implementation mentioned in section 2.1.3.4.

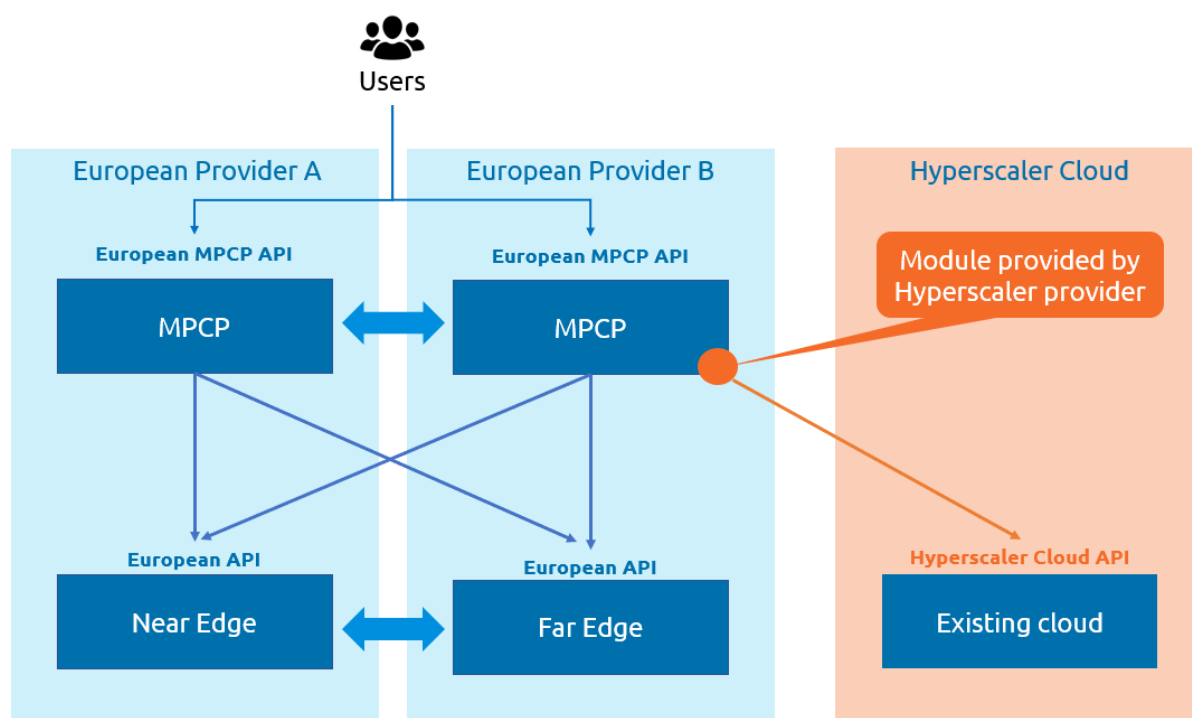


Figure: Multi-Provider and Cloud-Edge Control-Plane (MPCP) principles

In order to ensure the easy use of a federated European cloud, a uniform API framework is important for the development and maintenance of applications and services. Such frameworks exist today from every large cloud service provider as proprietary implementation and represents one of the success factors of cloud computing. In order to provide best possible user experience, a standardised, open source API framework must be able to cover cloud and edge as well as a broad set of providers. Already existing open frameworks should be considered and extended based on European cloud-edge requirements. Close cooperation with GAIA-X frameworks and federated services are crucial in this respect³³.

Basic elements for the API Framework are:

- API Portal to register and maintain API services
- Reference API Gateway to secure and route API requests
- Portal as user end point, collaboration and documentation
- Analytic functions for reporting and possible monetization

³³These standards should leverage the work initiated by initiatives like GAIA-X https://www.gaia-x.eu/pdf/Gaia-X_Architecture_Document_2103.pdf

- Integration in EU cloud Marketplace
- Integration in Multi cloud-edge Control Plane

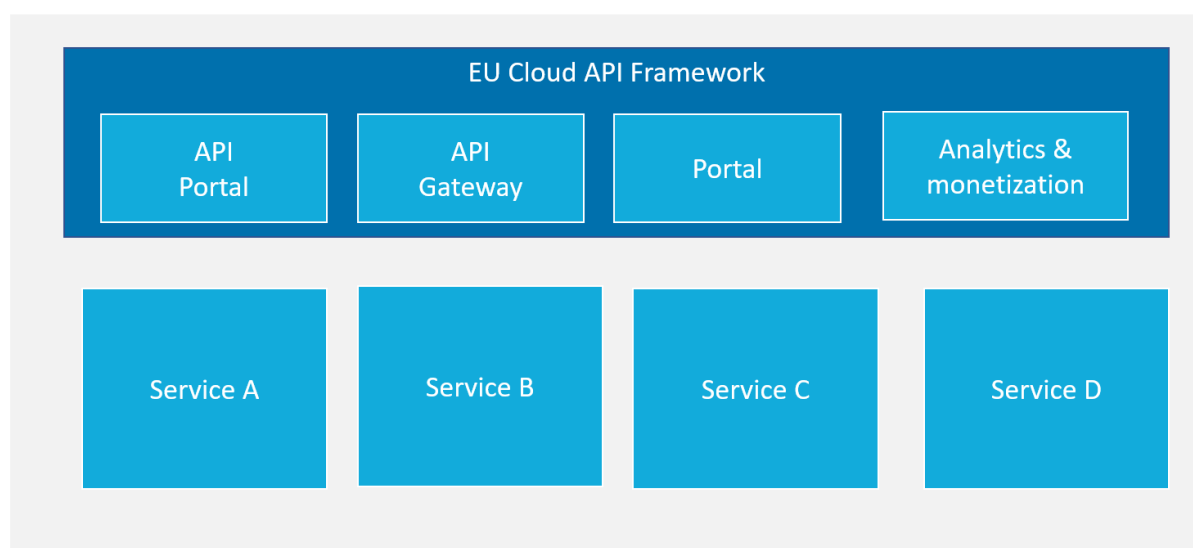


Figure: EU Cloud API Framework

The investment intends to cover the development of a European Multi Provider Control Plane and an API Framework based on existing open solutions and a reference implementation.

Required investment by 2025	150 M€
Rationale for investment	Market demand
Private:public ratio of expected investment	50:50
Is funding required to cover development, deployment, or both?	Both
Should investment be national or cross-border?	Cross-border

2.1.3.3. Federated European cloud marketplace

A common European marketplace for cloud and edge services would serve as a key enabler crucial to deliver on the EU Data Strategy's ambition to facilitate access to and fast-track adoption across Europe of cloud and edge service offerings that comply with EU regulation, European standards (including those provided for in Section 2.1.3.1 as well as user expectations in terms of data sovereignty, security, portability, or energy efficiency. This open marketplace concept would also strongly contribute to breaking down silos between national / sectorial markets across the EU, and accelerate integration across the continent, as this report calls for in section 1. The aim would be to serve the entire EU market, from public administrations to industry, including SMEs.

Such a marketplace would serve as a one-stop shop for cloud-edge applications from all providers that abide by European regulation. It would level the playing field and 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.

State-of-the-art user experience and interfaces (UX/UI), as well as standard APIs for providers would ensure smart integration and low adaptation costs for users and providers. An integrated billing and deployment model could also contribute to rapidly growing usage – while this will increase the marketplace’s complexity, federated approaches can simplify development.

The marketplace could be built to enable multi-tenancy: the service catalogue and technical foundations would be the same across Europe, but 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.

The marketplace foundations would be developed as open source, with open APIs, and integrate third party transparency for services such as verifying provider authorizations and certifications. Given the marketplace would, at least in its first years, be built and operate as a public-good, public-private collaboration is required to cover the build up and initial rollout costs. The investment cost provided for below would cover the development and integration of the marketplace technology framework (catalogue, user/providers interfaces and APIs, IAM, certification service, brokering service, reporting), an EU-wide reference implementation, as well as instantiation across the EU market, as well as the operating costs (including staff for brokering services) – where these are not covered by specific operators. Wherever it can serve as an accelerator, the marketplace should integrate standards as well as technology developed as part of GAIA-X federated catalogue framework³⁴.

Finally, early onboarding of a significant set of providers and users will also be key to accelerate the achievement of a critical mass of traffic to further its adoption, and leverage the lessons learned from leading global marketplaces to enlarge its user base.

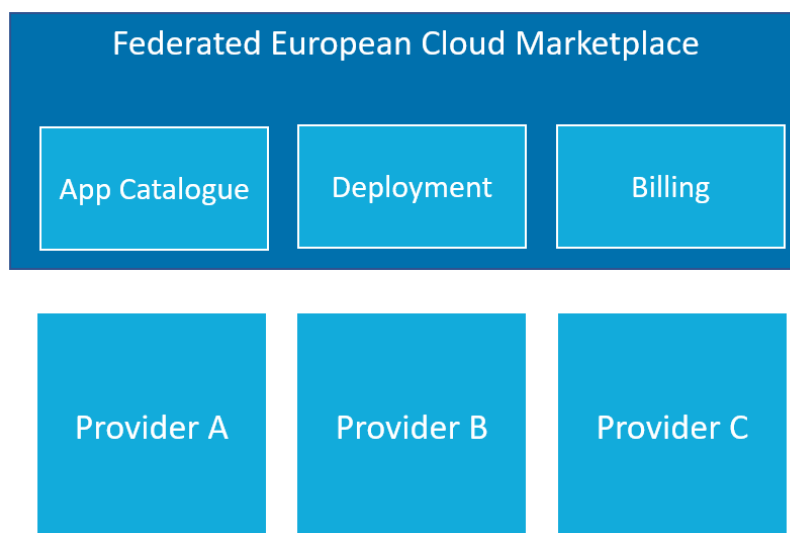


Figure: Federated European Cloud Marketplace

³⁴ https://www.gaia-x.eu/pdf/Gaia-X_Architecture_Document_2103.pdf

Required investment by 2025	100 M€
Rationale for investment	Market demand
Private: Public ratio of expected investment	50:50
Is funding required to cover development, deployment, or both?	Development
Should investments be national or cross-border?	Cross-border

2.1.3.4. Reference implementation for cloud and edge deployment – European cloud show case

This investment area will provide a real-world reference implementation of a European sovereign cloud infrastructure. Different investment areas will come together to show the power of joint development and cooperation across Europe. In order to enable efficient funding, this reference implementation should be transferred to a productive landscape at the later stage. This reference implementation can be use as a blueprint for deployment at large scale.

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

The diagram shows a possible setup, with two regional data centres, multiple availability zones, included the integration of “farther” Edges all the way to on-premise infrastructure, connected via interconnect.

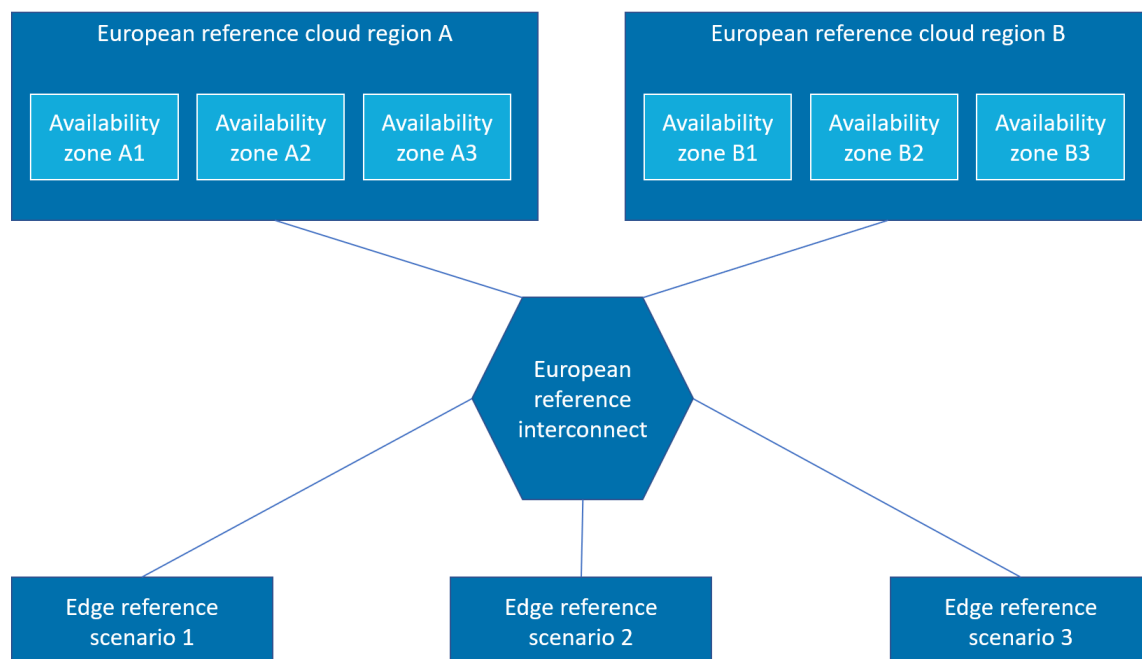
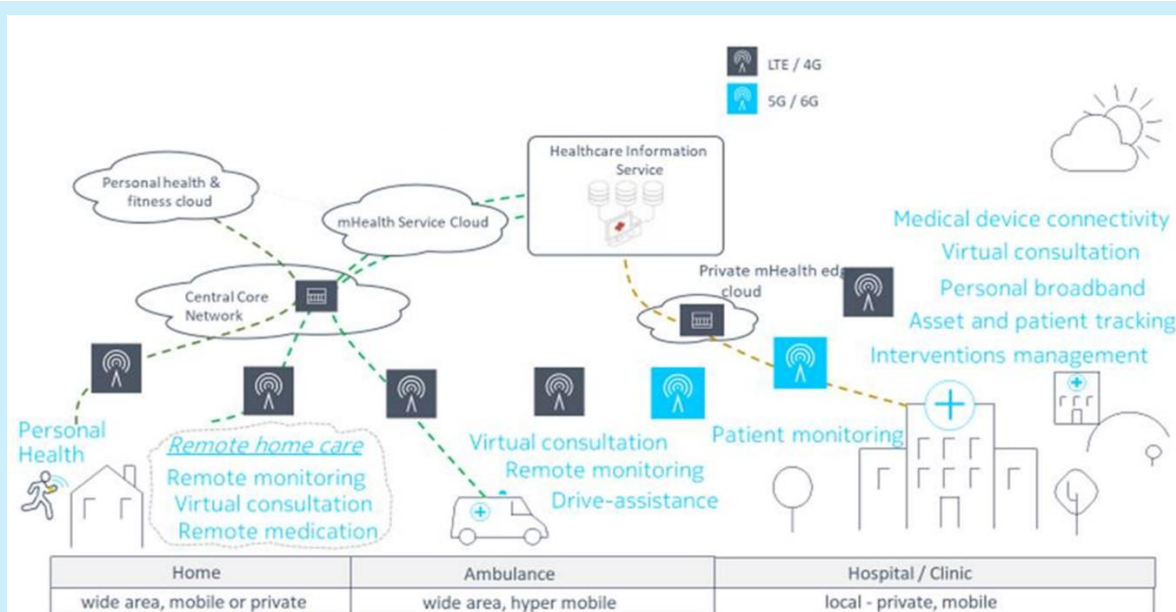


Figure: European next-generation cloud reference implementation

Required investment by 2025	500 M€
Rationale for investment	This is a form of public good. It is capital intensive and high risk, as the aim is to verify the compatibility of solutions developed according to common standards
Private:public ratio of expected investment	20:80 – public investment could be reduced by securing funds from the organization that will benefit from the end solution
Is funding required to cover development, deployment, or both?	Both
Should investments be national or cross-border?	Cross border

USE CASE: DIGITAL HEALTHCARE



Europe's increasingly ageing population has led to increasing as well as novel medical care needs. From diagnosis, prevention, monitoring, treatment of disease, investigation, anatomy modification... whether they are wearables or dedicated to a hospital department, medical devices offer many possibilities as they collect as information as they send back to their users.

Today, considerable volumes of data are already generated and collected by medical devices. Future medical devices will generate even more data and will require additional bandwidth, especially for highly consuming usages such as remote interventions.

Beyond additional infrastructures related to those Edge, data processing currently faces multiples challenges. Data collected through medical devices is highly sensitive. Currently, it is either processed and stored in manufacturers' cloud solutions, or on hyperscaler based solutions, which has two limits:

- Manufacturers do not necessarily have the expertise to cover all data usages, as algorithms design and data management are not in their core business, slowing the creation and deployment of such high-quality usages
- European citizen and governments aim for more transparency and sovereignty on their data.

Managing real time patient data require expertise and there are currently no global, sovereign, highly secured and resilient solutions that offer anonymisation or pseudonymisation techniques, consent patient management, high performance computing and other specific requirements (depending on the

instantaneousness need and the medical criticality). Providing European Edge & IoT solutions could cover the data collection, standardization, aggregation, and management to enable advanced use cases for improving European Healthcare

The following technologies are needed to achieve the aforementioned ambitions.

Data collection through:

- IoT platform creation and operation to take, store, aggregate and process data with service level guarantee.
- Edge algorithms with a trade-off between speed and algorithm performance, depending on the instantaneousness need and the medical criticality

Data preparation through:

- PaaS services: provide a data pipeline to collect, prepare, and process data for massive data computing, e.g., for research purposes
- Data platform: create a platform to gather, assemble, and expose data to create a European Health data space enabling massive data computing use cases for research

Underlying cloud capabilities:

- High performing network (e.g., 5G) to orchestrate edge devices and provide high bandwidth, low response time and high reliability
- Massive cloud infrastructures and performant underlying software to support the PaaS services and Data platform capabilities required to create the Health Data Hub

All those capabilities should encompass high security, data privacy, and integrity protection, aligned with special regulation and certificates

2.1.4. NEXT GENERATION DATA CENTRE INFRASTRUCTURE

The current maturity of data centre infrastructure is insufficient to allow the necessary growth of sovereign edge and cloud technologies in Europe. The European edge and cloud services can be built based on a combination of investment in three kinds of facilities.

First, new **Public Cloud data centres** buildout will be required in the region to cope with the increasing demand of electrical power expected due to massive adoption of cloud³⁵. These new data centre nodes in the region will reinforce edge capacity for the less latency-demanding applications especially in the markets where they are deployed.

Second, **Public Edge data centres** must also be developed as a capillary network of smaller facilities. Public edge data centres combine the benefits of proximity and ultralow latency of on-premise with the flexibility and scalability of public cloud and bring a much higher efficiency in terms of energy and resource consumption. This is because hardware utilization can be increased with respect to an on-premise/campus solution, as infrastructure is shared by a bigger number of tenants. Hosting several cloud providers in the same Public edge facilities would also reduce the consumption of energy in the transport network, as well as the operating and connectivity costs.

Third, **On-premise** or **on-campus** micro data centre built based on physical containers or purpose build edge hardware with much less power and requirements might be developed in cases requiring extreme privacy and/or latency.

In general, public funding ratio should be higher for those infrastructures that are shown to be more open, in terms of offering non-discriminatory access to several providers to the space, power and connectivity of the facility, as this will improve rollout speed, sustainability

³⁵ <https://www.cbre.co.uk/research-and-reports/Europe-Data-Centres-Q1-20>

<https://www.datacenterdynamics.com/en/opinions/why-europes-flap-markets-are-track-continued-growth/>

(power and resource consumption) and an operating efficiency that allows the region to focus efforts on innovation in other layers.

It must be noted that a parallel work, not in the scope of this industrial technology roadmap, to ensure availability of electrical power in the grid to feed the big cloud data centres is required, as it may be a burden to set up this kind of critical facilities.

2.1.4.1. Increased density of central-cloud and edge facilities

The Edge locations host:

- Network Edge Nodes (NEN), running Core, and in some cases fixed and/or mobile access, network functions; and
- Service Edge Nodes (SEN), running service applications.

The Core Network functions at the NEN are usually User Plane functions that perform the Local Breakout towards a SEN (i.e., allows the customer to reach the edge application), while the other Core functions (control plane) can remain in a Central Core Node. The applications at the SEN may be as well connected to other centralized applications and services for Non-Real Time functionality (e.g., Analytics) and for management functions. To achieve the benefits of the edge; that is, ensure latency, proximity, data privacy and security, NEN and SEN need to be collocated.

For this reason, the Core Central Offices of telecom operators can be a good starting point for deploying the edge as NENs (core network functions) are already available there, and these facilities are evenly distributed across the geography and with excellent connectivity with customers and other networks and service providers. Increasing the amount of SENs (edge locations) requires increasing by the same amount the NENs; that is, enlarging the capillarity of the Core Network and adapting the transport network topology. To leverage this network evolution, an edge rollout that uses the telco network for edge connectivity will usually start in the **Near Edge** (Core nodes, bigger facilities) and move progressively to the **Far Edge** (physical containers, aggregation nodes, closer to the customer) in a **Cloud to Edge** approach, following a supply-driven approach.

Alternatively, other edge providers may cover the earlier lower latency demand with an on-premise (private) or near-premise edge rollout, and may have, in order to interconnect the edge nodes to the cloud, to create a specific network or to rely in one of the existing public networks. This is an **Edge to Cloud** rollout approach, that follows demand starting in positions very close to the customer.

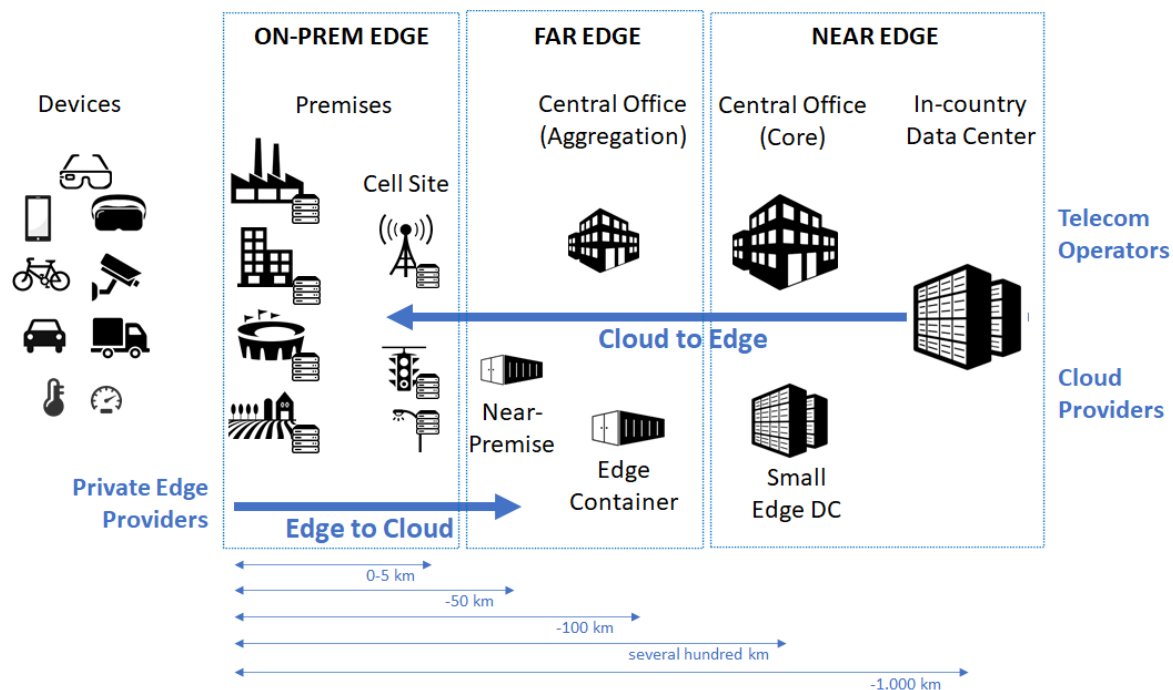


Figure: Expected evolution of edge cloud deployments.

The estimate below considers Far and Near Edge rollout. **On-premise** and **cell site** edge nodes are not included in the deployment estimate below as it is considered that they will be implemented on demand.

Type	Characteristic	Technical requirements	Non-Technical requirements	Estimated required rollout volumes
Cloud	Data centre less than thousand km far from device	<ul style="list-style-type: none"> - Wide area access - Multi-tenancy 	<ul style="list-style-type: none"> - Generic hardware and software to cover a wide range of use cases - Public 	2025 30-40 DC – exact number will vary depending on target size of DCs
Near Edge	Mini data centre several hundred km far from device	<ul style="list-style-type: none"> - Wide area access - Multi-tenancy 	<ul style="list-style-type: none"> - Hardware and software tend to be more generic to cover a wide range of use cases to increase multitenancy ratio (and efficiency) - Public 	2025 200 Near Edge nodes 2030 300 Near Edge nodes
Far Edge	Covering a certain area (<100km) and sometimes near-premise <50 km- to cover hotspots (e.g., shopping, business, industrial, event, farming or touristic areas)	<ul style="list-style-type: none"> - Wide area access - Extension of connectivity to local area - Multi-tenancy 	<ul style="list-style-type: none"> - Certain hardware and software configurations may be reinforced to serve specific verticals in the covered area - Public 	2025 6.000 Far Edge (w/ 4.000 Near-prem) 2030 14.000 Far Edge (w/ 9.000 Near-prem)

Type	Characteristic	Technical requirements	Non-Technical requirements	Estimated required rollout volumes
On premise	Close to data source (e.g. gateway, street light, traffic light, base station, road side unit) 0-5 km	In addition, it may require real-time connectivity to dedicated business systems	<ul style="list-style-type: none"> - Highly depending on vertical - Private 	There may be in the future hundreds of thousands of private on-premise edge nodes

On the **Cloud** side, the assumption is that, based on the current evolution, Europe will require at least an additional 350 MW of sovereign in-country cloud data centre infrastructure spread over Europe by 2025 in order to have a minimum percentage (10%) of the total IT power capacity provided by European data centre providers and meeting the best standards in terms of energy efficiency and operating performance. That computing capacity should be placed less than 1.000 kilometres far from most of the locations in the EU, through a combination of small and big data centres (5 to 20 MWs). Big ones would be recommended when feasible because of their higher economies of scale and pooling gains.

With regards to the **Near Edge** datacentres, in order to deliver at least 200 MW, a minimum of ~200 edge nodes would be required by 2025. As the Near Edge datacentre gives service to a smaller geographical area (typically, a radio of several hundred kilometres), the IT power requirement is assumed to be lower than in cloud (0,5 to 1 MW).

For some use cases, edge nodes may be required to be located at a distance below 100 kilometres from the customer, what is called **Far Edge**. Following the view presented by the European Commission for the next Digital Decade³⁶, edge computing capabilities will need to reach a minimum coverage of 10.000 nodes by 2030, enabling a ubiquitous experience of latency in the range of 5 milliseconds across the region. Around 6.000 nodes could be already in place at the Far Edge by 2025. A subset of them, 4.000, may be required to be closer to the customer (<50km), which is called **Near-premise**. Far Edge is composed of low-power nodes (30-100 kW) and may provide around 350 MW of IT power by 2025.

Although relevant to deliver the future demanded edge capacity, on-premise edge has not been included in the scope as it requires a deeper analysis of specific requirements of every sector: manufacturing, health, events, agriculture, etc and will be strictly demand driven.

The total new power capacity built by 2025, 900 MW (more than 200 MW per year), will help achieving the estimate of 80% of data processed at the edge by 2030, although, standalone, will not be enough to meet this target. It will contribute to stimulate the migration to the edge, kick-starting its availability and will have to be complemented with additional on-premise edge, not in the scope of this document as purely demand-driven. Central cloud is expected to grow linearly while the Edge cloud adoption rate will accelerate.

³⁶ "2030 Digital Compass: the European way for the Digital Decade", 9th March 2021: https://ec.europa.eu/info/files/communication-2030-digital-compass-european-way-digital-decade_en as part of Europe's Digital Strategy: <https://digital-strategy.ec.europa.eu/en>

DC power	<20 kW	<50 kW	30-100kW	0,5-1 MW	5-20 MW	20-100 MW
Cost/MW				9 MEUR/MW	7 MEUR/MW	
Average latency *	1 ms	2-5 ms	5 ms	10 ms	< 20 ms	> 20 ms
# per market	100.000s	10.000s	100s	10s	<10	Units

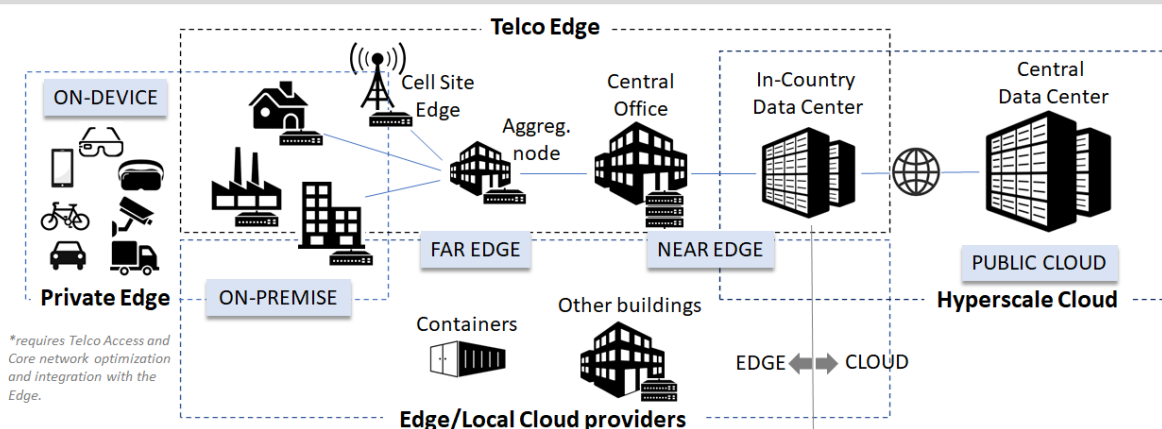


Figure: Characteristics of different types of edge and cloud locations

The required investment covers building conditioning, power, cooling, racks, cabling, security and maintenance, but does not include cost of land, hardware (servers, storage, network equipment) and software.

The investment in **Cloud data centres** is focused on deconcentrating capacities and achieving similar latency experience in cloud computing services across the EU (at this moment, countries like Spain, Portugal, Italy... do not host data centres for the big public cloud providers). It also aims at increasing sovereignty in the Cloud. Data sovereignty starts at the data centre, and this technology priority aims at making data centre facilities also accessible to European players who have lower CAPEX ability. Finally, there is a technology leap required specially to meet resource efficiency targets in these facilities. The public:private ratio applied to this investment will depend on the current availability of Public Cloud facilities in the market (e.g. 50:50 if there is already a certain density of cloud data centres, 80:20 if there are none or few).

CAPEX per MW increases when the data centre is smaller (7 M€/MW in a 10 MW data centre vs 9-10 M€ in a 1 MW one) due to the operational scale but may get lower (4-5 M€/MW) in the **Far Edge** where resiliency is not achieved by installing redundant systems and power generators in the data centre, but by grouping edge nodes in clusters backing up each other. In exchange, it requires a higher expense in edge-to-edge connectivity to provide an agile mutual back-up among nodes.

Edge nodes will receive a higher public funding ratio as demand still needs to be stimulated at the Edge while it is already existing in the Cloud. At the Edge, most of the rollout would be supply-driven, i.e. pre-empting demand.

Finally, as edge computing infrastructure is to be built worldwide, an accelerated deployment program could put Europe ahead of other regions in this new type of cloud computing that will become mainstream.

Required investment by 2025

Data centre infrastructure required by the EU up to 2025:

- **Cloud:** A combination of small (5-7 MW) and big (20-30 MW) data centres will provide around 350 MW: 2.9 Bn€³⁷

³⁷ Unitary costs have been provided by European companies that are building state-of-the-art data center as their regular business for European and non-European cloud providers.

	<ul style="list-style-type: none"> - Near Edge: 200 nodes (1 MW) delivering ~200 MW: 2.1 Bn€ - Far Edge: 6.000 nodes (30-100 kW) 2/3 of which will be 'near-premise', delivering 350 MW: 1.4 Bn€
Rationale for public investment	Capital expensive. A higher level of public funding is needed in the first years to pre-empt market demand, allow a first mover advantage for European providers, and stimulate demand and investment moving forward.
Private:public ratio of expected investment	30:70 during first 2 years (first 3 years for Far Edge), 50:50 onwards. The ratio may depend on required speed of deployment, and the openness of the datacentre infrastructure that is built
Is funding required to cover development, deployment or both?	Deployment
Should investments be national or cross-border?	National

2.1.4.2. Retrofitting of data centre facilities for improved energy efficiency and performance

The European edge and cloud infrastructure needs to be built based on the latest green data centre technology to deliver the energy and operational efficiency required to support competitive edge and cloud services. This efficiency will help the European edge and cloud providers to contribute to the European green targets. It will also channel resources towards innovation, further strengthening competitiveness and helping regain sovereignty on cloud technology.

Some energy efficiency solutions like high efficiency rectifiers, free cooling, cold water-based climate systems, hot/cold corridors, Computational Fluid Dynamics simulation and self-generation are mature and its application in new buildouts or in the retrofitting of network technical rooms is possible today but incentives and funds are not there to deploy it. Data centre facility providers should use them to replace legacy energy and cooling equipment and rearrange rack distribution, in order to meet the targets of energy efficiency and decarbonization.

Not addressing this topic can create a competitive disadvantage with non-EU alternatives. Europe can leverage companies and technologies supplied in the region.

Other technologies like immersion cooling or fan walls, or practices like district heating (waste heat reuse) are in an early stage of industrialisation. Although they are already applied in some areas and have great potential, it will require development, testing, and validation (covered in section 2.1.1.2).

Required investment by 2025	600 M€ ³⁸
Rationale for public investment	Market failure and capital extensive - Business cases on retrofitting existing datacentres have negative results and need high public support to happen. Moreover, energy efficiency of foreign data centre providers is higher and their investment capacities are inaccessible by smaller data centre facility providers in Europe.
Private:Public ratio of expected investment	20:80
Is funding required to cover development, deployment, or both?	Deployment
Should investment be national or cross-border?	National

2.1.4.3. Advanced data centre infrastructure management

Investments are also needed to develop advanced data centre management tools that would strengthen the operational efficiency of European cloud-edge offerings, contributing to their competitiveness.

There are several infrastructure management tools commonly used at data centres like

- Computer Fluid Dynamics (CFD) simulations to optimize rack layout in the data halls;
- Building Management Infrastructure (BMS) for real time monitoring of data centre installations, power consumption, and climate impact;
- Data Centre Infrastructure Management (DCIM) for monitoring, PUE management, operation, capacity, change space and network and Robotics Process Automation (RPA).

These tools are extensively used to avoid human errors in operation and monitor data centre working conditions. However, little progress has been achieved in taking advantage of the huge amount of data produced by these tools to improve data centre performance in terms of operational cost and energy savings.

Artificial Intelligence and Machine Learning give us the opportunity to analyse data centre infrastructure data and provide insight and guidance on actions to improve data centre operational performance as well as reduce energy consumption. AI and ML are key technologies to be developed and implemented for data centre infrastructure optimization. The application of AI/ML to the optimization of the complete data centre infrastructure and operations is a growing field of development where Europe can apply its existing skills.

Required investment by 2025	100 M€
Rationale for investment	Capital intensive / Pre-empt market demand
Private:Public ratio of expected investment	50:50
Is funding required to cover development, deployment, or both?	Development
Should investment be national or cross-border?	National and cross-border

³⁸ Estimated using historical data on data centre consumption in Europe, assuming that energy systems more than 10 years ago now require retrofitting. In 2010 Europe DCs were using around 400 MW. Rough estimate of the cost of retrofitting of 1.5M€ per MW (from a case on a single data centre)

See <https://www.datacenterknowledge.com/archives/2017/05/29/cbre-top-european-data-center-markets-booming-led-by-london>

USE CASE: AN INTELLIGENT PLATFORM FOR SMART WASTE AT THE CORE OF THE CIRCULARITY ECOSYSTEM

The European Union aims for recycling ratios to go from 30% to 65% by 2035. This target introduces a great challenge for local entities, waste producers, sorting plants, waste collection management and, of course, citizens.

The case involves the creation of digital business platform supporting waste management processes end-to-end, accessible to every stakeholder in the process (citizens, municipalities, public entities, waste management companies) independently of its size or digital maturity, with shared industry data and advanced intelligence capabilities.

The circular economy requires a fully integrated ecosystem with all the actors interconnected enabling the accomplishment of their different objectives:

- Enterprises: cost reduction and regulatory compliance as well as improving image, reputation and positioning
- Municipalities and local entities: answer to citizenship's demands, achieve recycling objectives and boost local economy
- Recycling companies: better recycling rates, cheaper materials, improve buyers trust in materials' quality and increased demand
- Collection companies: provide more and better services as well as optimize their resources
- Sorting plants: Increased transparency with processes optimization and automation
- Citizens: better knowledge of their role in recycling process, know the impact of their actions and have more information about the whole process

Instead of different vertical approaches, focus in the entire ecosystem must be set. However, heterogeneity of raw information is usually bigger than expected (for example IoT connectors, data models or connectivity).

A digital platform for smart waste is at the centre of all information flows between the different agents of the ecosystem.

Such platforms should enable a "data-driven" management approach that simplifies the complexity of the online raw data coming from the field (containers, waste meters, garbage trucks, routes) to all stakeholders.

It should provide real-time monitoring of the waste collection service: Connected fleets, containers and bins. Collecting KPIs in real time and applying advanced algorithms for route optimization. Integration of weighing information in the plant and evaluation of plant performance.

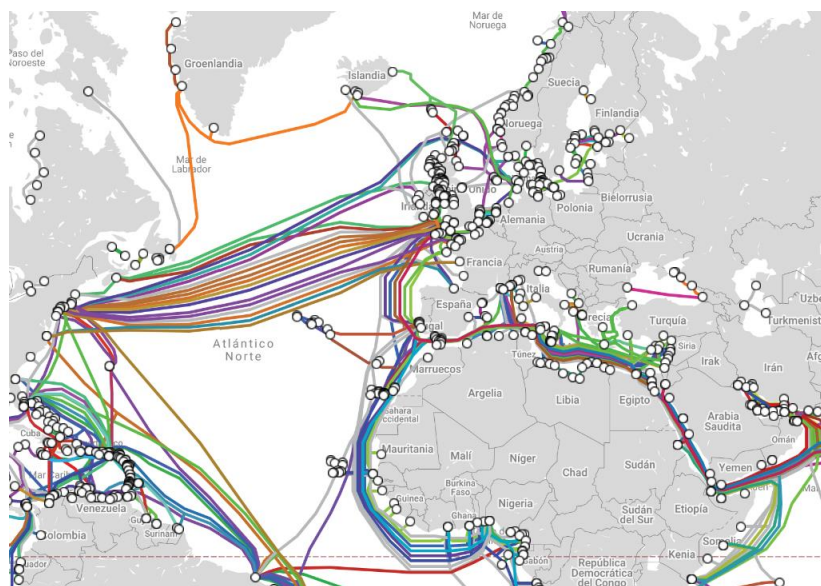
Key points of this platform-based ecosystem are:

- Defend the SaaS model as the way to democratize technology and enable a common intelligence
- Cloud architecture platform accessible for the entire ecosystem members, connecting physical world with virtual world
- Transparency provided by a single source of truth to all processes and members
- Advanced intelligence capabilities providing real-time route optimization, geo-referenced analysis and socio-demographic intelligence
- Work on standard models and systems based on API integration, reducing manual work and increasing transparency

2.1.5. NETWORK INTEGRATION AND INTERCONNECTIVITY

Already, 5G is being rolled out at high speed in the US and Asia, with Europe lagging behind. To take a lead in the digitalization era the EU needs to ensure that the platform for innovation built up by ubiquitous advanced 5G and fibre access networks, high-capacity fibre interconnectivity and the distributed cloud resources evolves in a coordinated way. The combination of these capabilities will ensure the competitiveness of European industry, not each part by itself.

The configuration and assurance mechanisms of the mobile network technology need to be adapted to deliver a secure and performing service, meeting the requirements like latency or bandwidth demanded by the edge and cloud applications. Due to the complexity of this dynamic configuration and assurance, orchestration and close-loop automation features, like the ones provided by network slicing, need to be developed and integrated.



2.1.5.1. Network service technology to ensure performance at the Edge

The availability of a safe communication path to/from the edge cloud provides a trusted environment that facilitates the adoption of public edge and cloud services. It may be a critical factor for some applications, handling sensitive personal or industrial data, to ensure that not only the data is stored in Europe, but also that the traffic to/from the edge node stays in Europe and is isolated at network level. Mechanisms to ensure such a control and isolation of data and traffic are key to ensure data protection and sovereignty requirements. The mechanism to couple the edge nodes and platform with the Mobile Network are being tested and standardized in bodies like GSMA, ETSI or 3GPP. This standardization process is expected to be completed by 2022 and its deployment will represent a significant effort of adaptation for the Mobile Networks. As depicted in the figure below, the user plane function needs to be implemented in each edge node to ensure a controlled local breakout, and that will require the adaptation of the corresponding transport network as well. Europe may lead this process setting up the first generation of edge computing optimized for Mobile users.

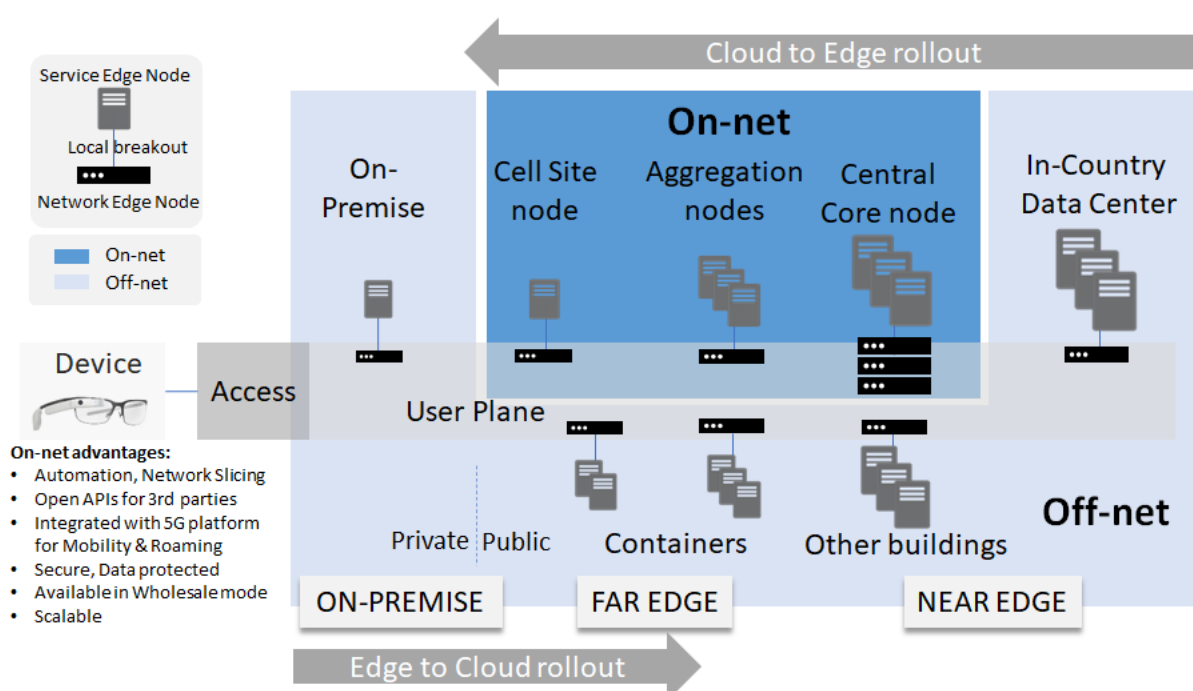


Figure: Local breakout (user plane function) required at each node to make the edge cloud continuum accessible to the customer with the right performance and security.

It will also require the development and deployment of mechanisms for security and isolation of data at rest and in transit that will set the trust environment required to enable the next data-driven industrial revolution. The development of Network as a Service APIs, supported by Software Defined Networking technology, will provide the means for automatic dynamic bandwidth allocation and latency configuration. Mobile Network building on 5G technology will play an important part of the total end to end network solution, providing functionality to ensure low latency and high reliability, but also ensuring break-out of traffic to edge clouds. Exposing mobile network capabilities through APIs to enable optimized utilization and configuration by Application Services provided on the edge cloud platforms is also essential.

Investment is required to complete standardization and development process of the mechanisms for Mobile network integration and their deployment in the edge cloud. It will be required to implement a number of these standardized interfaces and respective core functions in trusted European cloud services to provide “as a Service” offerings such as “5G-core-aaS” as backbone for Europe and worldwide IoT or automotive use-cases leveraging the edge infrastructure. By leveraging its advanced 5G and fibre network infrastructure, Europe

can become the first region to offer a uniform, controlled and high-performance edge connectivity to businesses, governments and citizens.

Required investment by 2025	650 M€ (see below)
Rationale for investment	The demand of latency, bandwidth, privacy and security cannot be addressed without the necessary adaptation of the telecommunication networks. Offering that at scale to customers, to support the region's digital transformation, will require automatic, on-demand and as-a-service mechanisms to monitor and control the network performance.
Private:public ratio of expected investment	30:70 (first 3 years), 50:50 4 th year onwards
Is funding required to cover development, deployment, or both?	Extension of user plane: 450 M€ Adaptation of transport network: 150 M€ Development of Network APIs: 50 M€
Should investment be national or cross-border?	National

2.1.5.2. Interconnectivity for European cloud and edge services

Cloud connectivity services – also referred to here as interconnection services – represent a key building block to handle the growing data exchange between the entities and meet user requirements in terms of latency, bandwidth, as well as security. The purpose of interconnection is to enable the envisioned federation of different European cloud providers at network level, as well as to connect metropolitan areas and edges to this cloud federation.

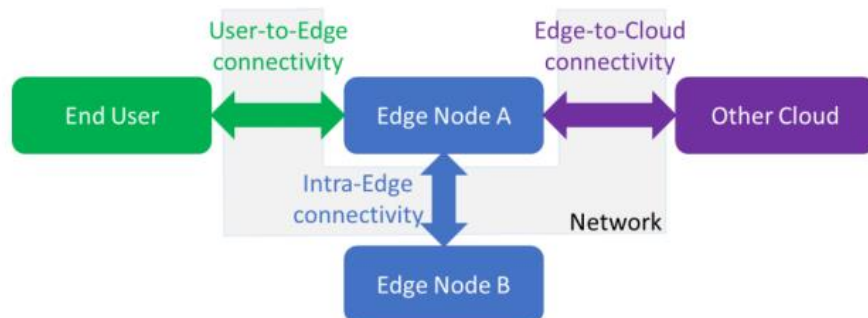


Figure: Investment in cloud connectivity services - interconnection services - is required to meet future demand and specifications for edge-to-cloud & edge-to-edge communication

Hyperscale cloud service providers have tremendous backbone networks in place and are directly interconnected with most relevant networks and are present at many Internet Exchanges (IXs) and Cloud Exchanges (CEs) across Europe. European cloud service providers need a similar high-performance communication infrastructure to facilitate federation and enable competitiveness.

The corresponding services can interconnect entities in different ways. Europe can leverage and expand its existing IX and CX infrastructure, as well as telecommunication networks, to meet future market volume and quality of service requirements. In addition, support can be provided to assist cloud and edge facilities in connecting to specific networks, according to market priorities. In any case, investment is needed to scale and strengthen cloud and edge connectivity on a continental, regional and local level, across Europe, in sync with forecasted deployments and usage of cloud and edge infrastructure (see section 2.1.4.1).

The R&D component of these investments should focus on developing standardized cloud connectivity services, enabling automation, orchestration and provisioning of those services, via standardized APIs and self-service portals on a European level. In parallel, Internet and cloud exchanges could be federated to provide networking infrastructure on a European level and extended to metropolitan areas, next to the near edges, complementing existing and future telecommunication networks.

Public-private collaboration can thus help make interconnectivity options secure, flexible and robust and will strengthen the European cloud and edge data centres, ISPs, and the carrier landscape by enabling a European distributed cloud platform.

Required investment by 2025	200 M€
Rationale for investment	Pre-empt market demand, anticipate future user requirements, and stimulate supply in EU regions prone to undersupply of interconnection (i.e. cloud connectivity) services.
Private:public ratio of expected investment	50:50
Is funding required to cover development, deployment, or both?	Both
Should investment be national or cross-border?	Both

2.1.5.3. E2E service orchestration and assurance across network and cloud

There is a need to develop and deploy a multi-vendor orchestration and assurance layer agnostic to the edge infrastructure, that can bring together and orchestrate applications and services across network domains including the edge infrastructure ensuring required service SLAs. Today, open orchestration and assurance solutions are not available – existing solutions are proprietary and closed. This provides an opportunity for European solutions to fill a gap, for the continents' users and globally.

To secure adherence to Europe's vision on data sovereignty and accessibility, it is important to secure control over the actors providing the multi-cloud orchestration and assurance layer that will combine cloud and network services. Consequently, mechanisms and interfaces need to be established to secure this performance across network and cloud in cross regional service realization. To roll out this type of orchestration and assurance capabilities with the right flexibility and agility, will require developing general AI technologies, network centric AI models that help deliver the E2E orchestration, as well as life-cycle management of AI models.

The accelerating cloudification of network functions and resources, establishes a new and fundamentally more dynamic reality for networks and network services. To this effect mobile networks are to a significantly higher degree than in the past dynamically adapting their topology and configuration parameters, as well as functional distribution, to secure levels of service performance and optimized resource allocation. To enable the application layer to interact with the e2e service orchestration layer, exposure of standardized API's (e.g. by TM Forum) is key for multi-vendor interoperability.

Required investment by 2025	150 M€
Rationale for investment	Create European competitive advantage
Private:public ratio of expected investment	30:70
Is funding required to cover development, deployment, or both?	R&D
Should investment be national or cross-border?	Cross-border

USE CASE: SMART AND SECURE URBAN MOBILITY

Municipalities across Europe and the world are more and more cautious of their attractiveness and increasingly embrace the ambition to become so-called “smart cities”. Among other challenges on this journey, it is usually found difficult to cope with traffic density and related effects such as air pollution, commutation time, insecurity, productivity loss and reduced quality of life. It is all the more challenging when we consider the situation of old European cities with their fixed (sometimes historic and protected) infrastructures that drastically limit structural upgrades and reconfigurations. In this context, essentially three ways open to old cities for improving traffic fluidity while maintaining acceptable safety and flexibility of urban transportation services.

One path is towards increased adoption of remote working and other incentives to individual mobility reduction (car ban, traffic fees, pollution fees, parking fees...). The second path is towards predictive/real time traffic optimization by enhanced connectivity of users, assets, vehicles and infrastructures. The third path is the enhanced use of the vertical dimension in urban transportation known as Urban Air Mobility (UAM). This use case would require strong collaboration between actors like city planners, transportation systems operators, passenger/traveller service providers, telecommunication service providers, road, rail, water and air vehicles manufacturers, computing specialists and security and safety specialists.

The above described paths are set in growing order of efficacy (& cost) and decreasing order of technological maturity. The following challenges will need to be addressed:

- The unequal access to high bandwidth low latency telecom services which are required to support remote working economy
- The inadaptation of existing infrastructures, vehicles and regulations to the adoption of Cooperative Connected and Automated Mobility (CCAM) uses
- The absence of an effective dynamic, safe and flexible management of urban air space, mobility and delivery systems

The above challenges can be suitably addressed by the development of the following capabilities:

- Secure scalable ICT infrastructures, leveraging on cloud and edge technologies, compatible with low latency high reliability lightweight cryptography and authentication mechanisms
- Distributed, explainable, privacy-preserving intelligent data collection, correlation, analysis, prediction and decision support systems. Such systems may leverage on quantum computing for highly complex predictions, for instance for traffic management.
- Integrate Urban (Air) Transport Management system, ensuring on the fly vehicle authorization, dynamic air space geofencing, collision avoidance and, vehicle interception tasks.
- Implement cooperative Intelligent Transport system C-ITS to provide trusted digital identities to smart connected transport devices facilitating the registration of secure elements and establishing secure communications among all components of the Smart Urban mobility system)
- Develop security behavioural analytics, leveraging deep learning, to monitor wireless signals including low latency communications and detect abnormal communications in V2X environments and M2V communications for threat anticipation.

2.1.6. NEXT GENERATION CLOUD-EDGE FOUNDATION INFRASTRUCTURE

The next generation sovereign European cloud infrastructure, which consists of hardware and hardware related software, needs to be open, highly efficient and covers cloud hardware components like compute and network as well as associated software components like firmware, operating system, resource orchestration, device management, security and monitoring.

The purpose of this investment area is to design several open replicable infrastructure blueprints (central cloud, near edge, far edge) which empowers to deploy and run efficient cloud and edge data centre, based on common engineering investments and individual deployment. Integration of GPU and low power CPU technology ensures the support of energy efficiency and workloads like ML and AI.

2.1.6.1. Cloud infrastructure control plane

The investment areas the present priority point addresses its efficient utilization and safe and reliable operation. The efficient utilization and distribution of the required resource represents a further success factor in the operation of a cloud infrastructure. Thanks to intelligent methods, provision and evaluation of telemetry, the utilization of the infrastructure can be increased many times compared to that of a typical enterprise data centre. The CPU utilization at traditional data centres is somewhere between 10-20%, which can be increased to 60-80%. This challenge is particularly critical for edge environments, where the infrastructure is often heterogeneous, widely distributed and with limited connectivity (hampering efficient real-time monitoring).

For efficient operation, it is necessary to collect a massive set of telemetry data which are kept under lock and key in conventional infrastructures and are sometimes also used for provider purposes. The aim is to make it possible that relevant meta data can also be made available to the user.

This investment focuses on the following areas, but is not limited to them

- Scalable hardware fleet/resource management
- Active workload management
- Deployment and lifecycle management
- Effective resource monitoring and scheduling
- Deep telemetry component monitoring
- AI driven predictive maintenance
- Meta data transparency
- Edge discovery, monitoring and self-healing

Development of open advanced hardware management tooling to ensure operational and energy efficiency and its competitiveness in reliability, performance, scale and cost.

Required investment by 2025	200 M€
Rationale for investment	Market failure
Private:public ratio of expected investment	50:50
Is funding required to cover development, deployment, or both?	Development
Should investment be national or cross-border?	Cross-border

2.1.6.2. Cloud and Edge hardware design, integration and deployment

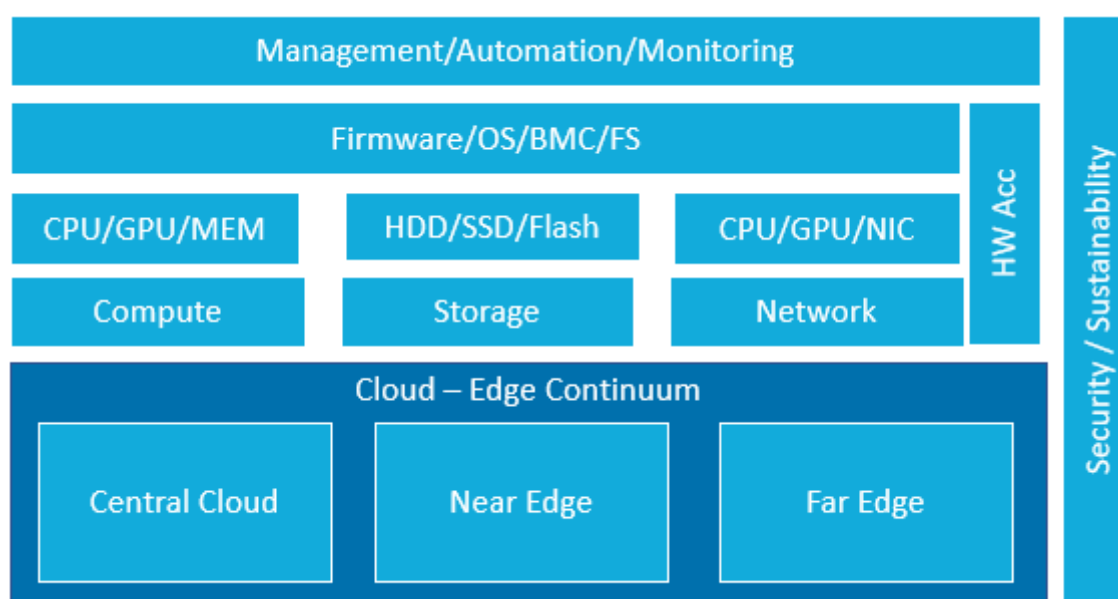
This investment area covers open design of technical specifications for hardware and the integration of existing and future components into efficient replicable cloud infrastructure building blocks. The investment includes but is not limited to computational design, special purpose hardware, confidential computing, hardware encryption and acceleration, storage, network (including smart NICs and NOS) as well as efficient packaging to ensure rapid deployment and low maintenance. It does not cover the development or manufacturing of microelectronic components like CPU, GPU, RAM, SSD).⁴¹

Infrastructure (server and network) represents as of today more than 65% of the overall data centre cost, making efficient design and operations a prerequisite to competitiveness. Currently, efficient and competitive cloud infrastructure technology is almost exclusively owned by market leading providers based outside of Europe, with proprietary designs and implementation. Each year, these players invest in the range of billions of dollars in order to increase efficiency and capacity. Only a closely coordinated private and public research and funding effort can provide alternatives.

An open reference, replicable architecture could be used to create an instrument that benefits European providers and the cloud industry at large. Leading providers could also feel compelled to disclose their infrastructure, which is also becoming more and more important with regards to provide assurances in terms of cloud security. Unknown built-in components and their firmware represent an ever-greater security risk, openness is urgently needed to avoid so-called backdoors, which can lead to unauthorized access.

Cloud and edge hardware effectiveness must be achieved from technologies at device level, network, power and energy management, and maintenance, while maximizing security levels. At component level, choosing high calculation-performing hardware such as GPU, FPGA and ASIC will ensure parallel processing or low latency calculation, perfectly suitable for real-time usages such as autonomous vehicles. These high performing hardware devices also offer hardware-based data encryption that offer a very high level of security from the beginning of the stack.

Network related hardware can also be optimized to offer more bandwidth with 400GE technologies, or to optimize the use of the available bandwidth with an adequate management between servers with improve network protocols like NVMe-oF, and smart network devices such as NICs (Network Interface Card).



⁴¹ See dedicated IPCEI on microelectronics https://ec.europa.eu/commission/presscorner/detail/en/ip_21_1343

Figure: Cloud and Edge hardware design, integration and deployment

Due to the scale of massive cloud and edge infrastructure, having an intelligent power and energy management is essential to optimize both the efficiency and the carbon footprint of our hardware components. On the one hand, advanced liquid in chassis and rack cooling technology would significantly reduce the energy required to lower hardware temperature and improve the lifespan of the hardware components. On the other hand, adopting low voltage power and high-power density technologies would maximize the performance out of minimal energy consumption, thus improving the energy/performance balance of the hardware components of the target European sovereign cloud and edge solution.

Besides material considerations, maintenance should be optimized as well and integrate open standards for remote management and low-touch maintenance, to increase the quality of the maintenance and its efficiency at scale across Europe.

Finally, security is a preoccupation at hardware layer as it is for every layer of our target stack. Beyond hardware-based encryption, low level security can be ensured by confidential computing, that isolates sensitive data while its being processed, making it accessible only to its program, and invisible for others, even for the cloud provider. Security can also be ensured at network level, with dedicated protocols that would enable encryption at network level, such as MACsec encryption.

To realize this ambition, the ratio of public to private investment will need to be higher (50:50) for design and integration than it will for deployment, however, deployment costs will be significant.

*Support to cloud-edge hardware **design and integration***

Required investment by 2025	300 M€
Rationale for investment	Capital intensive and public good (open standards) Creates competitive advantage for European industry
Private:public ratio of expected investment	50:50
Is funding required to cover development, deployment, or both?	Development (design and integration)
Should investments be national or cross-border?	National

*Support to cloud-edge hardware **deployment***

Required investment by 2025	6 Bn€ This investment would cover deployment of hardware for the data centres accounted for in section 2.1.4 (in country, near-edge and far-edge). The hardware should adhere by the open standards provided for in this section.
Rationale for investment	Capital intensive Creates competitive advantage for European industry
Private:public ratio of expected investment	70:30
Is funding required to cover development, deployment, or both?	Deployment

2.1.6.3. Hardware accelerated cloud native software for computationally intensive tasks on edge nodes

As bandwidth needs increase, commercially available off-the-shelf hardware cannot keep up, both in terms of performance, and power consumption. By the end of 2019, global mobile data traffic was around 40 exabytes (EB) per month and by 2025 we expect 160 EB⁴², with video-related streaming accounting for about three-quarters of the total. Multimedia streaming, gaming and AI, as well as networking are all applications that can benefit in terms of improved performance and reduced energy usage from direct access to optimized hardware, which in turn needs to be enabled through virtualization and containerization layers in a standardized and seamless manner.

Hardware acceleration on the cloud, and specifically on edge nodes is an important piece of the journey towards broad adoption of cloud technology, in areas with computationally intensive tasks such as telecommunications. The efficient and cost-effective execution of computationally intensive workloads can be facilitated by technologies such as, cloud native bare-metal execution (container technologies such as Docker) and orchestration (e.g, Kubernetes) of applications on bare-metal, or the direct access to dedicated hardware (e.g. GPUs, FPGAs or ASICs) optimized for the execution of specific applications (via SR-IOV, Single Root Input/Output Virtualization).

This technology can help further drive the global adoption of European cloud based 5G offerings, as well as secure the sovereign supply of 5G systems. Multimedia and gaming use-cases on the Edge Cloud, such as music or video streaming and gaming-as-a-service are only feasible given such accelerated computing capabilities. Finally, a plethora of upcoming AI use-cases will critically rely on the availability of hardware-accelerated Machine Learning and related facilities.

Required investment by 2025	75 M€
Rationale for investment	Create European competitive advantage
Private:public ratio of expected investment	30:70
Is funding required to cover development, deployment, or both?	R&D
Should investment be national or cross-border?	Cross-border

2.1.6.4. Edge-cloud native multi-tenancy

Centralization of computationally intensive tasks co-located at edge data centres can result in pooling gains and greater energy efficiency/reduced carbon footprint, by enabling elasticity of the Edge-cloud to facilitate consolidation of workloads across various vertical domains. However, such gains typically come at the expense of performance predictability, reliability, and security/privacy, as well as greater operational complexity and costs. These trade-offs are both a hurdle to successful market adoption and can also be detrimental to

⁴² Ericsson Mobility Report, <https://www.ericsson.com/491b06/assets/local/mobility-report/documents/2019/ericsson-mobility-report-q4-2019-update.pdf>

computationally intensive use-cases with strong latency requirements, as well as data protection considerations.

The goal is to secure “low-touch-management” capabilities, such as upgrade at scale, provisioning to enable fast roll-out, maintenance and emergency handling, and finally optimal workload distribution. Moreover, the performance and reliability of edge nodes when executing multiple computationally intensive workloads (bare-metal or virtualized) needs to be preserved, even while direct access to shared hardware resources is utilized. Workloads shall be secured and isolated including protection of all data at rest and in transit both internally and externally.

Edge-cloud multitenancy can be leveraged to enable higher occupancy rates associated with densification of 5G RAN and 5G RAN baseband processing, as well as Edge co-location of Enterprise workloads such as IoT data collection and processes, data analytics, application service provision, but also multimedia use-cases such as music or video streaming and gaming-as-a-Service.

Required investment by 2025	75 M€
Rationale for investment	Create European competitive advantage
Private:public ratio of expected investment	70:30
Is funding required to cover development, deployment, or both?	R&D
Should investment be national or cross-border?	Cross-border

2.1.6.5. Edge hardware / software disaggregation

Compared to legacy cloud infrastructure built on commercially available off-the-shelf hardware, edge cloud requires large cost savings and deployment flexibility to scale to significant levels. commoditization of edge hardware, starting with disaggregation, has the potential to create an open and competitive market for interchangeable parts that will help edge cloud achieve economies of scale.

Advancement in this domain requires open hardware infrastructure blueprints and reference architectures (see section 2.1.6.2 Cloud and Edge hardware design, integration), as well as open PaaS, IaaS and Container-as-a-Service (CaaS) at the network edge, software-defined networks for the data centre and for interworking between data centres, time-sensitive and predictable networking (see section 2.1.7). Collectively, these will afford the opportunity for cloud service providers to provision commoditised computing nodes at the edge data centre that can be used to host demanding workloads in terms of performance, reliability and security from multiple vendors and operators on the same (collocated) hardware infrastructure to manage and control multiple applications and customers. However, managing the evolution and complexity of this commoditized layer while ensuring high levels of performance, reliability and security are big concerns.

A disaggregated hardware/software architecture and related ecosystem of players has the potential to further drive the global adoption of European cloud based 5G offerings, as well as secure the sovereign supply of 5G systems. Multimedia and gaming use-cases on the edge cloud, such as music or video streaming and gaming-as-a-service are only feasible given a competitive disaggregated edge cloud environment.

Required investment by 2025	75 M€
Rationale for investment	Create European competitive advantage
Private:public ratio of expected investment	70:30
Is funding required to cover development, deployment, or both?	R&D
Should investment be national or cross-border? If both, specify what fits into each category	Cross-border

USE CASE: SECURED PLATFORM FOR PUBLIC SAFETY AND DISASTER RELIEF

Public safety networks provide mission critical communication solutions for police, fire and rescue departments, emergency medical services, and other critical government services. These types of services have specific communication requirements, and their network must be highly reliable and secure.

Public Safety agencies across Europe are on a journey to transform from legacy Narrowband public safety networks to Broadband Public Safety 3GPP, 4G and 5G- based networks: they will be able to leverage increased situational awareness thanks to this new capability of exchanging real time data, video and leveraging IoT. Data from IoT devices are supposed to help Public Safety forces to get a better understanding of an immediate situation and thus to react in a faster and more transparent way to an incident. However, there are only relatively few trusted platforms under governmental control for data collection and data provisioning in the EU today.

Given the lack of large-scale public safety platforms, many public safety stakeholders (e.g. volunteer fire fighters) are coming up with individual, hand-crafted solutions. These solutions are often not secure, not scalable and lack of interoperability in larger events, as other organizations have their own data repositories. The access rights and ownership of data do typically not belong to individuals but belong to organizations and roles inside organizations. These roles are generally dynamically assigned to officers. These roles are often only temporarily assigned and depend on the concrete function of an officer in a specific event or during an immediate situation.

In this respect "traditional" IT access and account schemes are not matching the need of Public Safety organizations. Implementing this use case would require overcoming legal, technical and organizational challenges.

- **Legal:** Today, any data collected is subject to the European General Data Protection Regulation. Thus, it has to be ensured that storage of any data and access to any data meets these legal requirements. This is by itself a challenging topic given the need to both strictly control and share individual data between organisations dynamically.
- **Technical: Access** rights to the Public Safety cloud platform are role-based and have to be dynamically adjustable triggered by tactical mission managers in specific events. Profile-based configuration, traceability of changes and mass reconfiguration of access rights for large-scale events are only some of the very demanding technical requirements. Thereby, the access of any individual user would have to be granted based on his dedicated role in an organisation for a certain event.
- **Organisational:** Most data is of interest for various Public Safety actors belonging to separate organisations, e.g. fire fighters and rescue services. The number of organisations and the structure of the organisations is extremely diverse (e.g. professional vs. volunteer, hierarchically managed vs. decentrally aggregated). The corresponding solution has to match all of these different setups in a suitable and operationally functional way.

Ideally, the solution has to be interoperable across borders and support public safety entities in all the EU Member States, to facilitate cooperation (e.g., fire brigades supporting another Member State suffering from forest fires, or in the event of any other natural disaster).

A starting point could be a shared public safety cloud platform (e.g., massive data shared by organizations within a city or selected data shared on a bigger scale). A solution approach could look as follows:

1. Propose a tailored cloud environment, which is reflecting the specific needs of IoT data and corresponding applications in terms of capacity and availability.
2. Harden this cloud environment to the specific security requirements of Public Safety related IoT data.

3. Propose a suitable connectivity scheme, which meets the needs of such data flows in terms of end-to-end security and quality of service and leverage the advent of 4G/5G based Public Safety networks.
4. Investigate on legal constraints and put a corresponding adjustable role-based access scheme in place, which fits the specific needs of Public Safety organizations and its users.
5. Demonstrate the benefit of shared data with an example application
6. Demonstrate the benefit of an example AI application, which will provide helpful guidance to Public Safety users based on learnings taken from existing data analysis.
7. A second, more advanced step may involve sharing selected data in a controlled way between two independent platforms on a case by case basis.

2.1.7. INFRASTRUCTURE SERVICES

For regionally and globally competitive cloud services, the European market must strengthen its offering of infrastructure services that match expectations for openness, transparency and interoperability. Many of these are already available as standalone or software services, but hyperscalers have the advantage of combining these services into an integrated offering. The absence of such a comprehensive European platform at scale prevents the market to compete. Alternatives can be found in a federated infrastructure using open standards, or a European collaboration (federative or otherwise) to create a solution of sufficient scale. The technologies below are needed to enable competitive European alternatives.

2.1.7.1. *Development of open standard/open source cloud software stack*

Most of current cloud offerings are based on some open source cloud, storage and network solutions (e.g. OpenStack, Ceph, Kubernetes). These solutions are dynamic, continually developing software platforms. No single firm is able to develop an entire cloud software stack on its own – thus there is a need for open source software components that will meet the needs of European cloud players/providers. The biggest issue to be developed and improved in the available open source platforms is related to scalability and interoperability. Scalability has to be developed:

- in the area of computing - for clouds with hundreds and thousands of compute nodes, in the area of storage - for network storage systems with capacity of hundreds of Petabytes,
- in the area of interoperability - with multiregion or multizone solutions for hundreds of edge nodes, in the area of networking to support hundreds/thousands compute and storage nodes, in the area of authentication, authorization, and accounting (AAA) with hundreds of federated entities.

The general purpose of this priority is to provide an open European cloud platform stack that reduces or removes dependency on 'as a service' infrastructure products from non-EU players. The availability of such a platform stack will enable European cloud 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. Additionally, a European effort in the open source cloud software development will decrease the risk of commercial takeover of open source software components (that would lead to proprietary closing of some software lines).

Following the cloud stack *standards* that are provided for in section 2.1.3, offerings of open source cloud software need to be developed and matured, to provide at least the following capabilities:

- Scalable, flexible, and heavily automated base compute and container services;
- Scalable, diverse and programmable storage services;

- Container platform integrations;
- Scalable interconnection *between* European clouds providing the same capabilities;
- Easy integration to the edge as well as on-premises;
- Security and protection services, leveraging the technologies outlined in section 2.1.2.

These capabilities will be able to sustain and take advantage of the PaaS services provided for in section 2.1.8, for a more complete stack.

The open source software development should be a continual process with the actual directions accommodated to evolving needs. An open and effective governance process should be introduced that will allow for selection of development priorities and will allow for rational distribution of funds.

Required investment by 2025	250 M€ Estimated based on 5 years of funding, 1 M€ per year per software project, based on 50 projects.
Rationale for investment	Technological sovereignty and autonomy
Private:public ratio of expected investment	20:80
Is funding required to cover development, deployment, or both?	Development
Should investment be national or cross-border?	Cross-border

2.1.7.2. First deployments of advanced IaaS/PaaS services

Hyperscalers provide extremely diverse virtual compute/cloud capacity and container services offering a single (proprietary) API from a multitude of locations. Containerization enables several applications to run on a shared O/S within a single device or server. Decoupling those dependencies improves portability, scalability and faster deployment, thus represent an essential service for the target offering. Europe has to focus on expanding footprint/coverage areas, as well as service diversity, preferably by adapting existing mature European solutions when possible. The purpose is to create equally distributed European cloud alternatives, therefore avoiding the current situation that limits the service options to non-EU platforms. Specifically, this addresses the lack of integrated open IaaS platforms. Current technology required for this is largely mature or will be matured by priority II.A.7.i - but often is not scalable, and will be accelerated by initiatives like GAIA-X. However, the actual organization and deployment of these platforms needs significant investments. Next to the data centre deployments for these services, an expansion is needed in terms of edge capacity for these IaaS/CaaS services.

The end objective is to realize at least 20-40 data centres hosted platforms as well as 100-500 edge nodes according to the principles laid out in Sections 2.1.4 and 2.1.5 in all Member States providing relevant and ubiquitous IaaS/PaaS services (compute, containers, databases, object storage, caching, big data services) that are otherwise not available in an integrated platform. This includes Life Cycle Management, orchestration and automation services for these platforms. These platforms function as building blocks for more advanced services and innovation – enabling European companies to build and market competitive and sovereign new cloud services. This is a collaboration between European companies providing relevant components (data centres, equipment, software, development and services).

While the European target will be to deploy across these 20-40 data centre platforms and 100-500 edge nodes as well as 6000 far edge nodes (in accordance with the projections from Sections 2.1.4 / 2.1.5 , public-private co-investment is most necessary for initial deployments that test and prove the viability of deployments. Additional funding/credits could be provisioned by public authorities to incentivize further deployment of an open European Cloud stack.

Required investment by 2025	100M€ made of : <ul style="list-style-type: none"> • 50M€ : first initial deployments for 3 in-country data centres, ~5 near edge facilities and ~80 edge data centres • 50M€ : subsequent deployments across the European cloud-edge infrastructure are assumed to be demand-led and are therefore not fully sized here, but further opportunities for public-private co-investment (0.1-2m€ per node depending on type) could be made available if public authorities which to incentivize deployments of a common open-source European cloud stack in Europe.
Rationale for investment	Market failure – providers will not individually take the risk of making initial deployments of a European cloud stack
Private:public ratio of expected investment	50:50 for first initial deployments
Is funding required to cover development, deployment, or both?	Both
Should investment be national or cross-border?	Cross-border

2.1.7.3. European “Telecom Cloud” reference implementation

Cloud and edge services are required for the deployment of technologies such as 5G Core and cloud RAN and are therefore strategic for achieving both global impact with European cloud technology, as well as European data sovereignty.

The telecom network with its widely distributed architecture, and ongoing evolution towards cloud native deployment, poses a unique opportunity to leverage both the strength of European telecom vendors, who are globally leading in providing cloud Native 5G, but also the global footprint of European telecom operators. 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, Open Source components, technologies required by some network functions such as hardware acceleration and the ability to sustain heavy computation workloads on the edge.

This cloud native edge will be able not only to credibly address Enterprise cloud use-cases but will also offer unique capabilities currently not provided by hyperscale cloud providers such as lower levels of latency, data residency or data transport optimization. Moreover, such Cloud Edge offerings, once successful in Europe, can be deployed globally. This cloud implementation for telecommunication and operator specificities would leverage a number of the priority technologies already features within the present roadmap.

- Compliant with EU data protection regulation

- Meeting telco industry standards and requirements
- Supporting technical, operational and data sovereignty principles
- Cost-effective facing the competition
- Multi-tenancy (Telco & Enterprise) for increased efficiency and reduced carbon footprint
- Flexible to accelerate the deployment of new features
- Monetizing the network, providing API to the BSS to automatically deliver added value services
- Automating the field operations
- Distributed CaaS to tackle edge for Telco requirements
- Baremetal provisioning adapted to thousands of nodes
- Optimized Life Cycle Management (LCM) for light weight and distributed nodes
- Hardware acceleration for computationally intensive tasks on edge nodes
- Edge Hardware / Software disaggregation
- Enabling seamless integration with other edge nodes

The objective is to achieve the alignment on a joint roadmap and perform related R&D to provide (i) the reference telecom cloud stack and make it available publicly but also (ii) the deployments of the initial instances and the necessary testing and certification facilities until the model reaches a critical mass and enough maturity.

Required investment by 2025	60 M€
Rationale for investment	Market failure
Private:public ratio of expected investment	50:50
Is funding required to cover development, deployment, or both?	Development
Should investment be national or cross-border?	Cross-border

In addition to developing a common telecom cloud stack, European telecom cloud providers will need to handle the deployment and the operation of this stack at regional & far edge. This will accelerate the transformation of the telecom ecosystem while avoiding the hosting of those critical Telco applications on a hyperscaler infrastructure.

Each operator would be able to implement and run the Telecom cloud software within their own networks. Alternatively, an association of European cloud providers, VNF vendors and operators could provide these cloud services for telecom operators. This scenario is credible because telecom applications do not require a service catalogue as rich as the one proposed by the hyperscalers to host IT applications. By extension, these cloud edge deployments could be used to host B2B use cases requesting sovereignty.

The responsibility of such telecom cloud providers would include:

- Ensure a sovereign cloud infrastructure for 5G compliant with telecom regulation
- Deploy the nodes across the region: technical environment, optimized hardware and the Telco cloud stack
- Ensure the management of Infrastructure (CaaS for Telco).

The telecom operators keep the management of the Network Functions (5G, etc.). The Network Function vendors focus on their core business, i.e., Network Functions software development.

Required investment by 2025	The investments required to deploy this software stack are already covered in the estimation provided in section 2.1.7.2. The exact amount will depend on the share of total edge nodes that will be deployed by telecom operators
Rationale for investment	Market failure
Private:public ratio of expected investment	50:50
Is funding required to cover development, deployment, or both?	Deployment
Should investment be national or cross-border?	National

USE CASE: MOBILE NETWORKS DRIVING CLOUD EDGE

5G is a cloud native platform, enabling edge deployment on dedicated cloud instances or 'slices' (up to the near and far edge) customized for the needs of each application, and supported by automation, programmability, AI and network exposure to 3rd parties. It enables new industrial applications interconnecting low-cost sensors and translating physical information into digital data at the edge. Moreover, 5G implements a public network compliant with EU data protection regulation, meeting telco industry standards, supporting technical, operational and data sovereignty principles, ensuring security and compliance with judicial authorities.

The result is faster growth in key industry sectors e.g. Manufacturing (smart manufacturing), Automotive (intelligent connected mobility, V2I/V2V/V2X technology), E-Health (Connected hospital, Home doctor, Remote assistance), Education, Tourism (Augmented and Virtual reality), Entertainment and Security (Smart surveillance, Smart C-room). Such applications may also be combined in a complex deployment of the required infrastructure, further emphasizing the need for a Cloud Edge integrated with 5G connectivity.

The European mobile network, with its widely distributed architecture, must evolve to adopt 5G and become cloud native, to enable the aforementioned industry and telecommunication use cases. This is a unique opportunity to leverage both the strength of European telecom vendors, who are globally leading in providing Cloud Native 5G, but also the global footprint of European telecom operators. These combined strengths can form the basis for a compelling value proposition in Cloud Edge, realized by transforming the mobile network into a network of widely distributed Cloud Edge nodes, implemented on standards based cloud technology, Open Source components, but also differentiating telecom technologies offering distributed high performance computing, higher bandwidths, lower latency, and higher resilience regardless of the physical location of the device.

The following technologies are critical in achieving this transformation:

- **Edge cybersecurity** (Secure Access Service Edge), must be built to ensure trusted architecture in collaborative edge. This includes a new network of security model that combines multiple controls such as Zero Trust Network Access (ZTNA), Cloud Access Security Broker (CASB), firewall as a service (FWaaS), data protection loss (DLP).
- As outlined in the section on Network integration There is a need to develop and deploy a **multi-vendor orchestration and assurance layer** agnostic to the edge infrastructure that can bring together and orchestrate applications and services across network domains including the edge cloud infrastructure ensuring required service SLAs. The development and deployment of mechanisms for security and isolation of data at rest and in transit that will set the trust environment required to enable the next data-driven industrial revolution. The development of Network as a Service APIs, supported by Software Defined Networking technology, will provide the means for automatic dynamic bandwidth allocation and latency configuration.
- 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. The disaggregation of hardware and software offers the opportunity for cloud service providers to provision commodity computing nodes at the edge data centre that can be used to host accelerated cloud-based RAN software for multiple operators, enabling Enterprises on the same (collocated) hardware infrastructure to manage and control multiple applications and customers (e.g., 5G RANs).
- The centralization 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. This opportunity is enabled by the higher occupancy rates associated with densification of the RAN and increased support for multi-tenant workloads.

2.1.8. PLATFORM SERVICES

Building on top of Infrastructure-as-a-Service, a diverse, open, and user-oriented European Cloud market must also provide Platform-as-a-Service (PaaS) offerings for application owners, developers, and authorized users. PaaS services should offer consumers a high-added value services such as a data processing pipeline; middleware and runtime capabilities to industrialize application development, deployment and integration; and optimized O/S

and containerization capabilities as on-demand services. The purpose of those PaaS services is to offer solutions that are created, packaged, set-up and supported by European providers for end clients to easily integrate by only having to load their data.

A strong offer of integrable high-end services, would maximize the European market's ability to generate services at large scale opening new revenue opportunities, reducing time-to-market and efficiently supporting innovation and commercial growth by enabling and accelerating the development of multiple differentiating use cases. But providing high quality platform services requires an equally qualitative cloud stack, skills to develop and package high-level solutions beyond IaaS capabilities, and a strong CI/CD pipeline automation to ensure proper instantiation and quality of services that will be available to customers on-demand. These PaaS services should provide the technical foundations to manage in a distributed environment (cloud or edge) Identity Access Management, Security & Compliance auditing, metering and contracting, standard open data exchange mechanisms, data catalogues, API catalogues as well as potential extended service catalogues (e.g. of algorithms), and AI environments.

Numerous small European players propose innovative platform solutions, but these actors and solutions are not fully at scale and cannot address the massive European demands. On the other hand, large European cloud providers are only starting to provide advanced services as they need to have a robust cloud stack to be able to build on.

2.1.8.1. End-to-end data pipelines and platforms

A priority service for the European sovereign cloud should be to provide a complete data pipeline to maximize the value of data, from discovering available data to complex AI based analytics. Being able to ingest data of different formats, from different sources will enable larger gatherings of data to create high potential data spaces. This data ingestion should be followed by adequate storage of the data, to retrieve it quickly and efficiently in order to facilitate its access for processing and usage.

Preparation capabilities such as aggregation, pre-processing when necessary, and normalization will be key to guarantee data quality for further usages, but also to respect national and EU regulations on data privacy, alongside data anonymization, traceability, and governance features. Preparation capabilities should also encompass data tagging features, to qualify data based on their content, whether the data source is text, image, audio, or video based.

As a highly valuable and sensitive asset, data must be protected and secured with trusted encryption algorithms, and proper access management, to ensure that only authorized actors can provide, access and use data they are allowed to.

Once data is properly stored, prepared and secured, high-value use cases can start to appear: build industry-specific data sharing ecosystems, leverage analytics of massive amounts of data to create value by crossing information, optimizing processes and activities through AI trained-models and pre-developed Machine-Learning frameworks.

Required investment by 2025	130 M€ ⁴³
Rationale for investment	Market failure – Existing end-to-end data pipeline are provided by non-EU hyperscalers while European data processing solutions are not scaled nor end-to-end
Private:public ratio of expected investment	20:80 for R&D / 50:50 for initial deployments
Is funding required to cover development, deployment, or both?	R&D <i>First deployments are accounted for in section 2.1.7.2</i>
Should investments be national or cross-border?	Cross-border for R&D and national for initial deployments

2.1.8.2. Middleware and Runtime capabilities enable large ecosystems

Additionally, Europe's target cloud and edge services offer should feature Runtime and Feature capabilities to industrialize application development, deployment and integration, as well as to enable rapid creation of applications and ecosystems.

Runtime services should offer quick and on-demand environment provisioning to enable sandbox innovations, developments, testing at low costs. By offering prepacked Software Development Kits (SDKs) and web/mobile application frameworks, runtime services would fasten the development of cloud-native applications fully capitalizing on cloud scaling and resilience capabilities. They should also provide deployment capabilities with a seamless continuous integration - continuous delivery - continuous deployment (CI/CD) pipeline that fully automate the deployment of applications, reducing time-to-market and improving applications quality with features such as A/B or "canary" testing that improve deployment rhythm and security.

Middleware are prerequisites to enable complex ecosystems of applications in the cloud or at the edge. They represent the bridge between infrastructures, or basic services, and high-value complex services or end user applications. Two types of middleware should be provided to the European market. Transversal capabilities would enable application integration and interoperability to support complex ecosystems of applications and interconnectivity both in and with the cloud. For example, API management and service mesh solutions handle interconnections between applications and are essential in micro-services architectures that will fully leverage cloud scalability. Besides interoperability capabilities, European cloud players should provide customers with managed databases with on-demand databases by handling infrastructure, database engine, licensing and management tools. Managed databases should provide relational and non-relational storage to support any type of data, and to enable every use of it for the data pipeline.

Required investment by 2025	120 M€ ⁴⁴
------------------------------------	----------------------

⁴³ This estimation is based on an investment covering 13 services: Data discovery, Data ingestion, Data preparation, Data anonymization, Data privacy management, Data traceability, Data governance, Data tagging, Analytics, AI training models, Machine Learning Frameworks

⁴⁴ This estimation is based on an investment covering 12 services: On-demand environment provisioning, - prepacked Software Development Kits (SDKs), web/mobile application frameworks, seamless CI/CD pipeline, API management, Service mesh, Managed relational databases, Managed non-relational databases

Rationale for investment	High quality services and standards set by hyperscalers must be proposed by European cloud providers to offer value to their users and ensure adoption
Private:public ratio of expected investment	20:80 for R&D
Is funding required to cover development, deployment, or both?	R&D <i>First deployments are accounted for in section 2.1.7.2</i>
Should investments be national or cross-border?	Cross-border for R&D and national for initial deployments

2.1.8.3. Managed Databases and custom operating systems for industrialization

Managed databases and custom operating systems (O/S) are also key components to quick start customers' projects in the cloud and edge allowing them to leverage pre-package optimized functions.

Databases are essential for a vast set of applications but can be complex and time-consuming to setup, especially for non-Databases experts. Managed databases are databases that are provisioned, configured and maintained by cloud providers, while clients only have to load their data and connect it to their applications. By simplifying and automating database management, they quicken app developments as clients do not waste time on setup and can directly focus on value-added developments. They are already a standard in Hyperscalers services but should be proposed in an EU offer as they are very demanded and are key to ensuring end-to-end data sovereignty.

From cloud facilities to far edge devices, the need for aligned, interoperable software providing compatible features will be essential to create highly scalable and integrated ecosystems. O/S is key to ensure a common foundation, as it is the bottom layer and encompasses all basic functions required by upper software. To maximize interoperability from edge devices to cloud data centres, EU should thus develop its own O/S. In addition, edge device storage capacity is limited, it is key to optimize and minimize as much as possible the size of the software deployed on them. In that matter, deploying containers and custom O/S will require less capacity on the edge device, reducing its cost devices, and will optimize cloud performance, while guaranteeing an end-to-end control on the devices that will be essential for security and sovereignty purposes. In addition, having custom O/S allows for creating or optimizing dedicated features that are essential for embedded systems in European industries.

Finally, to address the needs of far edge environments where the physical devices are the most resource-constrained, additional specialised components will have to be developed, namely edge-compatible container management & deployment, on-site computing extension capabilities or Real-Time Operating Systems (RTOS).

Required investment by 2025	50 M€ ⁴⁵
Rationale for investment	EU custom O/S are necessary to maintain an end-to-end sovereignty up to edge devices where security is a top concern
Private:public ratio of expected investment	20:80 for R&D / 50:50 for initial deployments
Is funding required to cover development, deployment, or both?	R&D <i>First deployments are accounted for in section 2.1.7.2</i>
Should investments be national or cross-border?	Cross-border for R&D and national for initial deployments

USE CASE: REAL-TIME MONITORING AND ANALYTICS FOR FUTURE ENERGY MARKETS

In 2019, the European Union agreed on a new energy strategy to achieve carbon neutrality by 2050. One of the most important measures is redesigning the electricity market in EU.

This objective involves the promotion of development and greater integration of distributed energy resources (DERs), such as distributed renewable generation, storage jointly with the active participation of demand.

As an example, there are currently + 350k wind turbines in the world, and the market is expected to grow to + 10% CAGR. Operation of these wind farm networks, combined with variability of weather conditions introduce complexity and risk of unpredictability in energy production.

The “electrification” of demand and the integration of DERs represents an important technological challenge since it involves a very high and heterogeneous number of points that will be connected to the Medium Voltage Low Voltage distribution network or directly at the point of consumption. Key challenges are to:

- Connect a greater amount of renewable energy, in particular in the distribution network. For example, real-time monitoring of signals from thousands of sensorized and connected wind turbines in wind farms in different countries with 250k measurements per hour on average
- Integrate the flexibility of the demand in the electrical dispatch and operation of the network
- Provide technological support to the electrification of demand, in particular electric transport
- Integration of weather forecast from third-party sources
- Growing ratio of distributed energy resources (DERs) introducing variability in both energy demand and offer
- Geo-located visualization layer in real time of the different wind farms that integrates the different sources of information

Considering the extension and diversity of the producers and consumers ecosystems the solution is needs to comprise:

- the creation of a platform that efficiently integrates the entire ecosystem,
- the development of solutions that allow optimizing the management of distributed energy assets,
- the development of equipment that allows automation of the infrastructure with high cybersecurity standards, and

⁴⁵ This estimation is based on an investment covering 5 services: Managed relational databases, Managed non-relational databases, Dedicated Cloud O/S, Dedicated Edge O/S, Real-time O/S

- the definition of interoperability standards that ensure the scalability of the model.

Key drivers:

- Modular and flexible cloud architecture platform that enables the connection of all the assets
- SaaS model as the way to democratize technology and enable a common intelligence
- Geo-located visualization layer in real time that integrates the different sources of information to improve production forecasting by applying advanced analytics
- Massive sensorization for monitoring the entire ecosystem raw data (wind farms, consumers, DERs, electric vehicles, etc.).
- Leverage big data, advanced analytics and artificial intelligence.

2.1.9. APPLICATION & DATA SERVICES

2.1.9.1. *Pan-European data sharing platforms*

Data sharing between economic stakeholders is a source of value creation and global competitiveness that remains largely underexploited. It enables a step change in existing or creation of new data-driven use and business cases, especially those leveraging artificial intelligence solutions - that require a large volume of high-quality industrial data to deliver all their value. European public and private organizations are a source of many attractive data, examples of which include: Earth observation data (Copernicus initiatives), manufacturing industry data, healthcare data, mobility, or scientific data in many areas like genome research.

The quick and effective set up of data spaces – an ecosystem of public and private organisations, standards and technologies that enable shared value creation via the exchange of data and data-driven solutions – is key to exchange data seamlessly between economic stakeholders and create value. Data spaces will open up access to public sector and private sector data sets and provide impact and business opportunities especially within business verticals where Europe has a strong position. Some initiatives have already been launched to meet industry needs and agree on data sharing standards, such as the GAIA-X and IDSA framework.

Creating – that is, innovating beyond the existing global state of the art - the highest layers of data infrastructure and imposing standards that abide by European values on the underlying infrastructure and on data exchange could provide a fast and cost-effective way to maintain European users' sovereignty over their data.

At the end of the day, European data sharing spaces will connect a multitude of individual data spaces across organisations, industrial sectors, and geographical boundaries. To take full advantage of data spaces the target is now to invest money to realize these ambitions and allow development and deployment of those data-driven services to end-users (governments, business, citizens). This includes data platform, governance, management, interoperability and standards for secure and effective data sharing between organisations. Europe is at a pivotal moment to show its leadership in development and governance of data sharing platform at international level with the creation of a trusted data sharing infrastructure. They should comply with European laws and regulation in terms of data protection and sovereignty and reflect common European values and principles including openness, privacy protection and interoperability.

These platforms should also allow data transfer related fees if a producer want to change its data to another repository. Moreover, data producers and services providers should be able to share their data (with or without remuneration) while keeping their property so that value is not captured by a small number of stakeholders.

European cloud and edge services should therefore integrate the technical foundations to cover the transversal needs for the European data platforms, assuming massive distribution of data and of data process execution. This could be compared to a control plane for EU Data management, pivotal to agile and compliant handling.

It is then obvious that the development of this pan-European data platform and some of the related data sets will have to be available to all European cloud and edge users so that these users do not have to leave European infrastructures to access this data. It must be users' choice to decide how to handle their data leveraging the technologies outlined in the present document (e.g. PaaS, infrastructure, cybersecurity), including their localization (regional, national, European or worldwide). Pan-European data space solutions should ensure the appropriate level of transparency, sovereignty and security of data to enable

trust and confidence in data sharing, also providing clarity on their exposure to non-EU extra-territorial laws.

However, data platform creation represents a huge investment and effort for European companies with unclear short-term return on investment. Entry costs - investments, operational costs and lack of clear business model for a relevant data platform - could therefore prove prohibitive for private stakeholders. That is why public intervention is essential to prime the pump and allow private players to exceed certain thresholds.

A first part of the investment must go into developing common good technologies and tools that should be sector agnostic (data marketplaces...) as well as data interoperability standards. No private players will be able to invest into these elements at necessary scale without a strong involvement of public bodies. The actual investment would mean supporting the development of a data platform solution that:

- Integrates the cloud service and API standards provided for in section 2.1.3.1 and the PaaS services outlined in sections 2.1.8.1 and 2.1.8.3, particularly those enabling data ingestion, indexing, discovery and tagging. This should be done in way that provides ability to access datasets for any European cloud or HPC infrastructure, check the metadata associated with data to be able to respect its attributes, transform data if needed, store it, and transfer it, use it or manipulate it in a secured and standard manner. The resulting solution should give all means to business to build any type of data-driven applications on trusted infrastructures without depending on the infrastructure provider (e.g. European or non-European) to deliver that trust.
- Contains software modules for contracting on the fly, clearing houses, invoicing, payment systems, that will enable stakeholders to reach a self-sustained economic model and that act as a referee in case of conflict. This should provide an effective mechanism for revenue collection for data platform operators.
- Allows the conduct of research around mesh technologies.
- Builds efficient data repositories at the level of 50 PB each with potential of scaling up.
- Ensures standard technologies between all the dataspace, ensuring that they will connect to each other.

Support should also be provided for the cloud infrastructure/ecosystem to develop the compliance models to allow a full control of the parties based in the EU of the data collecting and exchanged therein, as well as effective revenue collection models for data providers.

Secondly, public-private collaboration and co-investment is needed to kick-start the first use cases in vertical ecosystems and fast track adoption by a critical mass of data users and data producers in order to make data sharing economically self-sustainable in the long-term. This should build on the action plan announced by the European Commission as part of the EU data strategy. These investments would cover:

- Development of several pan-European data platforms data spaces across different industry verticals that will be built on this data platform technology.
 - These dataspace can only start with public funding at the beginning.
 - Support should be provided specifically to create the data catalogues and the semantic associated.
 - Technology specific to the vertical should be developed
 - Redundancy (including geographic redundancy) may be required

- API or connectors should be specifically created for any stakeholders in EU being able to easily connect to the EU cloud infrastructure, notably for SMEs, with warranties on respect of European values of data and protection on extraterritoriality laws.

Finally, the regulatory environment should enable users to develop, deliver and market their data-driven applications easily (see Section 2.2).

Required investment by 2025	For technical foundations (data sharing platform and toolbox: 1 Bn€ For deployment in verticals, to enable adoption until critical mass of users is achieved: 500 M€
Rationale for investment	Market failure / Capital expensive
Private:public ratio of expected investment	20:80 for R&D to develop data sharing toolbox 50:50 – for deployment
Is funding required to cover development, deployment, or both?	Both
Should investments be national or cross-border?	Both development and deployment should be on cross-border collaboration between national players

2.1.9.2. Application services enabling development of edge use cases

Achieving a mass uptake of cloud and edge by European stakeholders will depend on the ease and speed with which the market can develop value driven applications and services, with a seamless integration into a cloud to edge infrastructure.

It is therefore critically important to encourage the development of such application services and facilitate their exposure in open marketplaces to deliver the foundations upon which added value use cases will be delivered at the edge. Some of these application services may be of use across multiple sectors of the European economy, while others may be more appropriate to service the needs of some specific sectors and industries.

A non-exhaustive selection of these application services would be:

- Edge-compatible supply chain management platform (most appropriate in the industrial and manufacturing sectors)
- Machine Learning (ML) and Artificial Intelligence (AI) based analytics hosted on the cloud or at the edge, for example to enable a faster, more accurate and trusted medical diagnosis in hospitals
- AI object detection powered by visual computing technology (most appropriate for automated vehicle applications), enabled by edge computing and 5G
- Shared hub for design collaboration (whether cloud or edge based) to enable collaborative design across multiple industries/organisations, for example leveraging Augmented Reality/Virtual Reality (AR/VR) technology and digital twin modelling
- Remote operations of robotic tooling (whether in medical or industrial applications), enabled by a combination of 5G, edge computing, AR/VR and digital twin modelling.
- Blockchain-based federated learning frameworks, enabling privacy-preserving federated learning and training while providing trust and auditability of the

federated learning ecosystem. It can also be combined with AI/ML and AR/VR technology for more advanced learning and training use cases

- Microgrid management platforms, hosted and operated at the edge, to enable the efficient management of renewable energy sources in remote locations or small energy grids

The list of application services powered by cloud and edge which would provide significant value to European stakeholders is virtually limitless. The common factor between these different applications is that cloud and edge serve as both an accelerator and a facilitator for the delivery of these application services to their consumers, improving the performance and increasing the availability of these services.

But while the development of these services can generate a significant and tangible value for the European economy, it will also require extensive investments in R&D and engineering to materialise these ambitious applications and in marketplaces to make them widely available within and across the different verticals. The financial intervention of public institutions (via IPCEIs for instance) is therefore an unavoidable prerequisite to making the development of these applications accessible for private sovereign stakeholders.

Required investment by 2025	150 M€
Rationale for investment	Market demand – Capital expensive
Private:public ratio of expected investment	50:50
Is funding required to cover R&D, deployment, or both?	Both
Should investment be national or cross-border?	Cross-border Investment as primary focus. Some selected national investment possibly due to geography or specific vertical use case.

USE CASE: SUSTAINABLE TRANSPORTATION

The European Union aims to be carbon-neutral by 2050, an objective that is also at the heart of the European Green Deal. More and more companies across all industries have set net zero objectives between 2028 and 2050. Transport represents almost a quarter of Europe's greenhouse gas emissions and these targets are a challenge to many companies in transportation, for example the shipping industry as indicated in this use case.

Facing increasing mobility needs for citizens and goods require the need of higher performance and efficiency while at the same time reducing energy to achieve net zero targets.

- Improvement of vessel performance is one of main transformation pillars.
 - Fuel consumption is key in the vessel performance - >50% of the total cost
 - Significant time and effort investments on vessel maintenance
 - Reduce harbour time while maintaining quality and decrease turn-around time
- Edge is critical to train algorithm on the vessels due to poor connectivity & network quality in the sea with data centres based on the countryside.
- The next generation cloud-edge solutions covered in this paper would enable:
 1. Creation of a central vessel resource optimization platform for big data analytics and Artificial intelligence leveraging on HPC Edge for network and connectivity reasons while shipping across the oceans to enable:
 1. Transparency on technical status information
 2. Fuel consumption benchmarking
 3. Better turnaround time of vessels
 2. Reducing harbour time by using cloud prescriptive and predictive analytics in an integrated and combined solution with SET, 3D-model, Digital twin
 3. Behaviour analytics and simulation integrated with engine engineering
 4. Intelligent port systems and dynamic vessel flows for improved routing and scheduling
 1. Usage of route and speed calculation algorithms taking into account criteria: weather, traffic, priorities, etc.
 2. Real-time adaptation to the ordering of priorities
 3. Smart management of calls for service vessels

2.2. Enablers of success

The developments in infrastructure and technology listed above will more effectively achieve European strategy goals if be supplemented by enablers of success. These include supporting clear regulations as well as targeted programs. A European framework ensuring the effective function of the market, based on clear and enforced principles is a cornerstone for achieving our overarching goals. This section outlines the many, sometimes complementary, forms that such policies and regulations could take.

2.2.1. Synergies with existing private and public initiatives, notably GAIA-X

It is of utmost importance that the upcoming development of the EU Cloud Federation, which will include a cloud rulebook as well as a marketplace, should rely on the GAIA-X initiative as the basis. The standards, reference architecture and rules that are currently developed within GAIA-X need to be reflected in the upcoming Federation, to avoid creating two initiatives that – despite their identical vision – would not sync together due to different rules, governance etc.

2.2.2. Programs that align with digital sovereignty objectives should be supported or reinforced by the European Union and Member States.

The European Union and Member States must make the connectivity and data management end to end a key objective by setting up and promoting programs that reinforce edge and cloud sovereignty. For example, European Institutions could establish a certification of “European data sovereignty” to guarantee to customers that certain sovereignty requirements are met along the entire value chain, from data acquisition to storage and transmission. It can also promote incentives to keep European data in European clouds dimensioned to offer any 5G service in any European country with integrity. Such benefits are appreciated by Enterprises world-wide and can be made available with the same level of guarantees to leverage Europe’s position as a trusted host.

Europe can also play a more active role in encouraging innovation and research. For example, the EU could encourage collaborative Research and Innovation by providing sufficient (co)-funding for AI and key enabling technologies through Horizon Europe. A joint research and innovation strategy would also be helpful to federate efforts and investment, therefore building synergies with other vertical and horizontal initiatives.

Moreover, European and national public administrations should serve as drivers of demand, through early adoption of solutions that champion the principles outlined in the present investment roadmap.

2.2.3. Regulation that enables the growth of European cloud and edge industry

Addressing current market needs, including the ambitious connectivity targets for fibre and 5G, and it is clear that we need a shift of regulatory paradigm to succeed in that endeavour. The EU’s Recovery and Resilience Fund combined with the new Digital Decade 2030 targets and the planned update of the Industrial Strategy, present an opportunity to align Europe’s industrial policy vision with the right competition policy and regulatory environment to secure a much stronger future for the European economy and society.

Cloud and edge are an integral part of technologies such as Cloud Native 5G Core and Cloud RAN, which represent strategic opportunities for achieving both global impact with European Cloud technology, as well as European Data Sovereignty. The European regulatory framework must be adapted to ensure that it is conducive to investment in Cloud Native 5G. The following are potential aspects that can drive competitiveness and investments:

- There is an urgent need to release available 5G spectrum for potential investment, remove deployment barriers in the form of permits, and alleviate related site costs. Overall avoid extracting value from the industry through very high spectrum prices that hinder investments. Reserve prices in particular should be based on the estimated value of spectrum in its best alternative use, rather than on the estimated willingness to pay of auction bidders.
- Align competition policy approaches with the industrial policy vision favouring scale through pan-European and in-market consolidation, (especially when a proposed merger could potentially create a 'front runner') and therefore also potential investments in infrastructure.
- For an interconnected sovereign EU cloud ecosystem to scale, industry efforts alone are not enough. The public sector needs to generate key demand and needs to drive demand for the to-be-developed EU cloud standards in public tenders. And this needs to be done at all levels, EU, national, regional and local level.
- The success of a European-based cloud infrastructure depends on its scale and better functionality, benefits which will attract users from existing solutions. Another potential benefit would be to seed the European cloud and edge with data. Regulation reinforcing trust in data and data services (data transparency, data protection, algorithm explainability) would be helpful.
- The promotion of regulatory sandboxes, given the complexity of all actors involved would facilitate an understanding of what does and does not work. It would also provide legal protection for the stakeholders involved.
- Regulation or public funding should be technology neutral, and not be used to push the market toward a particular structure, with skewed results, even if such a market structure may be considered advantageous in certain contexts.
- Lastly, acceleration of Infrastructure investments can be achieved via National Recovery and Resiliency Plans and horizontal funding such as a fixed price purchasing e.g., feed-in tariffs for renewable energy or tax rebates like the 'super deduction' scheme announced by the UK recently that allows companies to offset 130% of the value of their investments against their tax bill for a limited period.

3. Overview of technology priorities (2021-2025)

The technology priorities amount to a total public-private investment need of ~19 bn€ by 2025

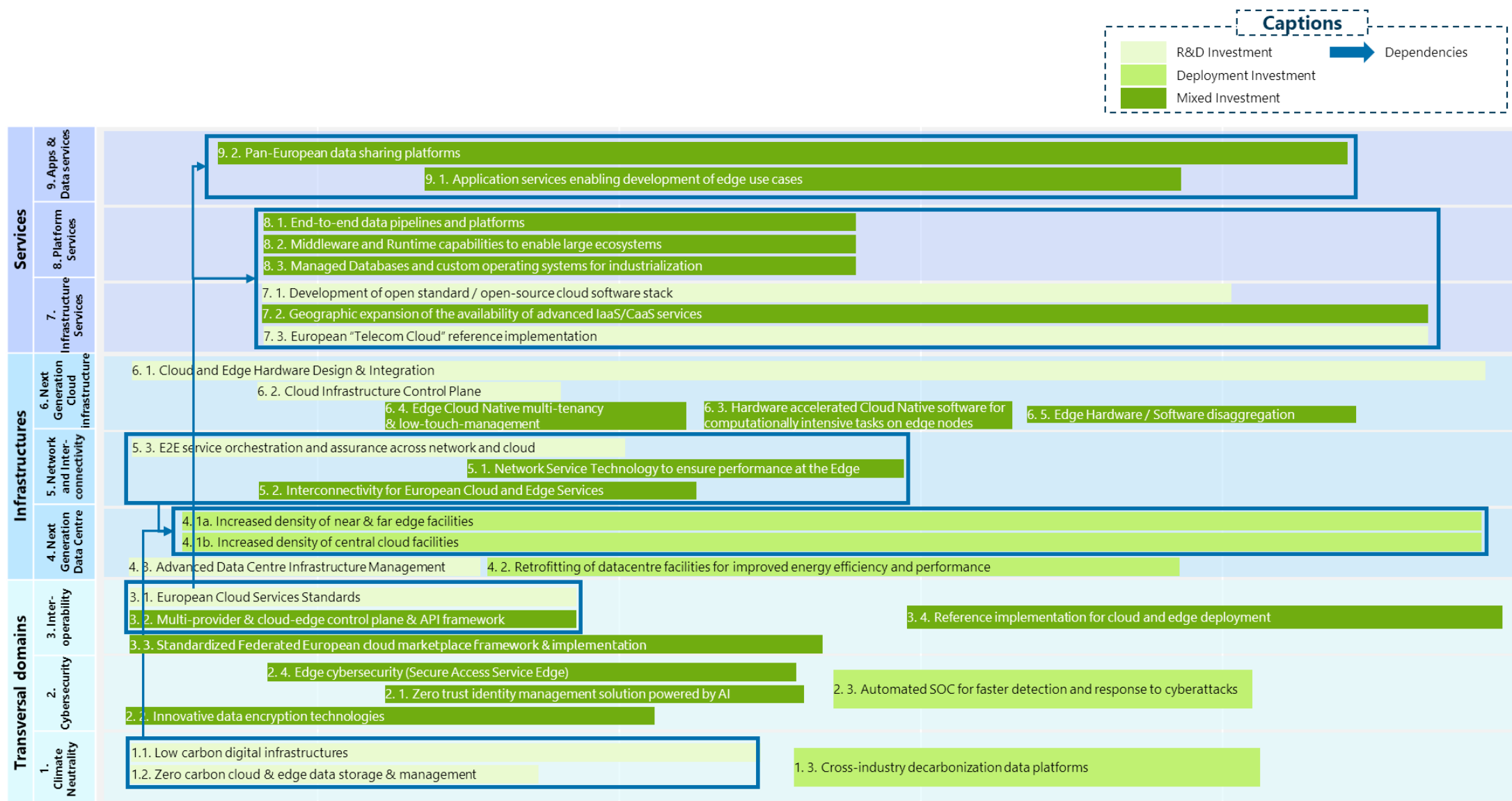


Become the global leader in transversal domains				Renew and expand infrastructure foundations across Europe				Enable sovereign and sector-specific services to end-users						
1	CLIMATE NEUTRALITY AND RESOURCE EFFICIENCY	200 M€	Low carbon digital infrastructures	4	NEXT GENERATION DATA CENTRE INFRA - STRUCTURE	Cloud: 2,9 Bn€ Edge: 3,5 Bn€	Increased density of cloud facilities	7	INFRA-STRUCTURE SERVICES	250 M€	Development of open standard/open-source cloud software stack			
		100 M€	Disruptive technologies to enable zero carbon cloud & edge data storage & management				Increased density of near & far edge facilities			60 M€	European "Telecom Cloud" reference implementation			
		100 M€	Cross-industry decarbonization data platforms			600 M€	Retrofitting of data centres facilities for improved energy efficiency and performance			100 M€	First deployments of advanced IaaS/PaaS services*			
2	CYBER - SECURITY	500 M€	Zero trust identity management solution powered by AI			5	NETWORK INTEGRATION AND INTER-CONNECTIVITY	650 M€	Advanced data centre infrastructure management	8	PLATFORM SERVICES	100 M€	End-to-end data pipelines and platforms	
		500 M€	Innovative data encryption technologies including quantum safe encryption	200 M€	Network service technology to ensure performance at the Edge			130 M€	Middleware and runtime capabilities enable large ecosystems					
		250 M€	Automated SOC for faster detection and response to cyberattacks	150 M€	Interconnectivity for European cloud and Edge services			120 M€	Middleware and runtime capabilities enable large ecosystems					
		270 M€	Edge cybersecurity (secure access service edge)	6	NEXT GENERATION CLOUD-EDGE FOUNDATION INFRA-STRUCTURE	200 M€	E2E service orchestration and assurance across network and cloud	50 M€	Managed Databases and custom operating systems for industrialization					
3	INTER - OPERABILITY AND MULTI-PROVIDER SERVICES	50 M€	European cloud services standards			200 M€	Cloud infrastructure control plane	9	APPLICATION & DATA SERVICES	1,5 Bn€	Pan-European data sharing platforms			
		150 M€	Multi-provider and cloud-edge control plane & API framework			6,3 Bn€	Cloud and Edge hardware design, integration and deployment*			150 M€	Application services enabling development of edge use cases			
		100 M€	Federated European cloud marketplace			75 M€	Hardware accelerated Cloud Native software for computationally intensive tasks on edge nodes							
		500 M€	Reference implementation for cloud and edge deployment			75 M€	Edge Cloud Native multi-tenancy and low-touch-management							
						75 M€	Edge Hardware / Software disaggregation							
Overall:		2 720 M€		Overall :		14 825 M€		Overall :		2 360 M€				
Estimated private contribution:		1 125 M€		Estimated private contribution:		7 950 M€		Estimated private contribution:		640 M€				
Estimated public contribution:		1 595 M€		Estimated public contribution:		6 875 M€		Estimated public contribution:		1 720 M€				

* conditional on deployment of open standard hardware / open-source cloud stack

NB: only activities that require some form of public investment are listed here. Certain deployment phases will be fully demand-funded

Example of roadmap and service dependencies for deployment (2021-2025)



This roadmap view is a tentative example that will need to be revised when designing and attributing the investment plans for each technology. Other interdependencies are likely to appear between or within priorities. The duration of developments is not to scale.

4. A vision for European cloud-edge in 2030

The appropriate application of cloud-edge technology has the potential to be the enabler of truly transformational thinking over the next decade. This will come as the focus of digital technology application increasingly shifts from doing things more efficiently, effectively, quickly and cheaply, to thinking differently, acting differently and tackling problems in ways that were not previously possibly.

Underlying infrastructure and data management will appear more homogenous as standards and interfaces enable frictionless trusted ecosystems, no-code solutions and automated deployments - Compute capability will move towards being a true utility that is increasingly orchestrated by artificially intelligent system management engines. Artificial intelligence will not only enable self-configuring and self-healing infrastructures; it will also support the dynamic creation and control of access authorizations to context sensitive data catalogues. A new paradigm of truly adaptive hybrid computing and **cognitive cloud and edge** will emerge.

Security will of course be paramount but will become more automated and intelligent supported by the consensus mechanisms and immutability offered through Distributed Ledger Technologies. The scaling up and use of underlying infrastructure must be done in a way that contributes to the solution for decarbonization and the carbon neutrality objectives.

Some examples of data-enabled solutions that are expected to mature by 2030 include:

- **“Edge manufacturing”** enabled by large-scale and distributed additive manufacturing. The use and impact of digital twin technology will accelerate as we close the loop of “physical to digital” representation and “digital to physical” rendering.
- **“Swarm computing”** characterized by intelligent edge devices automatically and securely collaborating to perform complex tasks. Increasingly this will include nanotechnology components that will lead to the emergence of so-called **“smart dust”**. The mass deployment of tiny, smart, edge devices raises all kinds of security, ethical, sustainability and other environmental challenges that must be addressed.
- **“Human Task Augmentation”** will be made possible with collaborative robots (including exo-skeleton suits⁴⁶), advanced human machine interfaces and interactive augmented reality visualizations. In particular, we expect the HMI (Human Machine Interaction/interfaces) as the bridge between the digital and human worlds to mature, not only proximity & motion sensing or conversational interfaces through natural language but also neural interfaces and computers that can understand emotion, with enormous potential in Healthcare or as Assistive technology. Such technologies also raise ethical questions which have to be addressed.
- The advent of true **“Quantum supremacy”** will allow the solutions to what are currently considered to be intractable or even impossible problems. A new world of hybrid classical and Quantum computers will open the way to discovering new materials and drugs and new levels of process optimization. But they will also demand new approaches to security.
 - Fully **“Automated business operations”** will see a further shift in the nature of work and in the nature of business value and perhaps even macro-economics.

⁴⁶ Wearable mobile machine.

- Continual progression towards “**General AI**” will open up a whole new realm of possibilities but will also further strengthen the imperative of digital ethics, trust and transparency. We will be faced with the kind of challenging questions that as humans we often struggle to deal with. The quest for digital systems to “think” more like humans, will see the development of **neuromorphic or “brain inspired” computing** capable of emulating the neural structure and operation of the human brain. This will lead to new algorithmic approaches that can deal more effectively with the uncertainty and ambiguity of the real world.

All these trends not only demand scalable and reliable infrastructure to deal with huge volumes and complexity of data, they demand new approaches to balancing transparency, trust and security. There need to be new models for fairly managing the derived value from data – ones that recognize and address the externalities of digital such as carbon impact and societal divides.

As data volumes reach zetta-scale levels and society’s dependence on the integrity and availability of digital solutions reaches the level of critical national infrastructure, more formal governance and interdisciplinary work will inevitably be required at a number of levels. Appropriate protection of economic and wellbeing interests will demand a collective and extensive public-private approach to digital technology R&D&I and operation.

Maintaining an acceptable level of parity with other leading global states will require further investments at European level to foster significant public-private collaborations that will deliver against the vision laid out in this section.

