OPEN STRATEGIC SOVEREIGNTY

The pathway to a trusted European cloud-edge ecosystem

MARCH 2022

Capgemini Invent has contributed towards the contents of this report strictly for the purpose of studying evolving policies in Europe regarding data sovereignty.

Capgemini Invent is not authorised to, and does not provide, legal, regulatory or compliance advice.
All advice given and statements and recommendations made in this Report by **Capgemini Invent** are:

- provided in good faith on the basis of information provided by **Vodafone**, **Vodafone's** third parties and/or otherwise generally available or known to **Capgemini Invent** at the time of writing; **Capgemini Invent** has not independently verified the accuracy or completeness of the information provided by **Vodafone's** third parties;
- and are made strictly on the basis that in no circumstances shall they constitute or deemed to constitute a warranty or undertaking by **Capgemini Invent** as to their accuracy or completeness. To the full extent permitted by law, **Capgemini Invent** disclaims any liability arising out of or in connection with this report (including but not limited to any reliance, action or decision based on the report).

CONTENTS

FOREWORD

Cloud technology, and increasingly edge technology, is a key strategic enabler for Europe's digital and green transitions. It ensures resilient, scalable and energy efficient processing capacity across Europe. Its adoption drives future European competitiveness and innovation, including by unlocking the full potential of AI, data sharing and low latency 5G applications.

Yet, the adoption of cloud technologies in Europe remains too low, especially among small and medium sized companies. Also, to date, the cloud market is largely dominated by a few US technology companies, or "hyperscalers".

Europe is, rightly, sensing it is falling behind – just as it has on many other innovative technologies.

This report, in partnership with Capgemini Invent, analyses the dynamics currently at play within the cloud market, to better understand the challenges and opportunities Europe faces. Also, it sets out a number of recommendations of what can be done to compete and lead on a global scale.

The good news, as per the findings of our report, is that there are reasons for optimism provided action is taken now to build the right kind of cloud and edge computing ecosystem. In particular, with the right policy and regulatory frameworks in place, our continent could generate up to 14.5 additional percentage points of cloud adoption by 2030 relative to the baseline forecast, and benefit from a 576-billion-euro opportunity thanks to increased data exchange and digital collaboration within and across organisations.

The less good news is that there is a growing trend towards too simplistic and binary actions aimed at "technological sovereignty" in the context of cloud and data, even diverging interpretations of how to achieve such objectives, which run a real risk of stymying this value generation. As underlined in this report, it critical that the EU adopts a unified and coherent approach that adequately balances the various interests that are at play, and ensures the adequate precision required to achieve Europe's legitimate sovereignty interests without undermining its longer-term competitiveness and innovation. The report specifically recommends focus on three actions:

1. ***Develop a common understanding on what strategic technological sovereignty means for European cloud and edge computing, thus preventing a fragmented approach.***

2. ***Create a harmonised, fit-for-purpose regulatory framework for cloud-edge services.***

3. ***Adopt a strategically 'open' approach to technological sovereignty, favouring targeted regulation over exclusion.***

To be clear, a significant majority of EU-based organisations surveyed as part of this study consider that any blunt ban on non-EU providers would significantly impact their bottom line. Here there could be some useful learning from its past efforts around the 5G security toolbox, launched by the European Council in 2019. The ambition of EU-wide, risk based and vendor neutral standards and certification – based on shared European values and interests – was and continues to be the right one. Yet, as also correctly pointed out by the Council of Auditors, Europe's shared interests have to date been ill-served by the continued divergence in interpretations of risks and of measures related to 5G between EU member States, as well as by the far too slow process of putting in place the necessary common technical standards and assurance systems.

In short, Europe's technological sovereignty – just as its response to the climate and energy crisis, or to the pandemic – requires a pan-European response, one that addresses real risks with targeted and proportionate regulations that are no less trade-restrictive than necessary. Importantly, it also implies embracing the value of collaborating with like-minded countries and entities that share European values and are able to demonstrate essential equivalence with EU laws, thereby leveraging regulation to ensure healthy, contestable, and fair markets. In contrast, vague requirements that 'sovereign' providers demonstrate 'immunity from non-EU law' are not only likely to be inconsistent with a number of principles of EU law and the EU's WTO obligations, but also would not deliver the outcomes European customers are asking for.

Of course, since we commissioned this study, the question of sovereignty has taken on a new urgency, in light of the devastating war in Ukraine and the threat to European security that this implies. Building a strong economic and industrial base, reducing strategic dependencies, and increasing EU capacity via targeted investment will all be central to ensuring European resilience necessary to withstand current and future threats, including those in the digital domain. These sentiments underpin the conclusions of the European Council leader's summit on 10th March and the Versailles Declaration that the EU must invest further in digital technologies in its drive to reduce strategic dependencies.

We commend this new sense of urgency and shared resolve. The cost of European long standing inaction – across a number of sectors – has not served the EU's collective interests well. But just as Europe is right to strive to address the alleged naiveté that has led to some of its strategic dependencies, it should not replace it with another naiveté about what is required for European businesses and employers, small or large, to be successful in the real world.

The European Single Market should remain open to trusted service providers that meet its regulatory requirements, protecting fundamental European rights and values whilst also meeting the needs of EU customers. It is this approach that will propel the EU's twin transitions of digital and green transformation.

JOAKIM REITER

Chief External and Corporate Affairs Officer,
Vodafone Group Plc'

EXECUTIVE SUMMARY

Cloud-based data solutions have played a crucial role during the COVID-19 pandemic by enabling remote-workforce collaboration and productivity, and fostering business agility, continuity, and resilience. As cloud and edge computing continues to proliferate, concerns relating to data sovereignty have gained prominence in Europe with the EU's 2020 Data strategy, the ECJ's 2020 Schrems II verdict, and more recently the announcement of national cloud policies.

Different sets of policy schemes and certifications are emerging across EU Member States. For example, certain Member States are choosing to emphasise the need for 'immunity from non-EU legislation', when the EC has itself decided to extend the free movement of data principles to jurisdictions that demonstrate adequacy in terms of data protection, like the UK or Switzerland. Such discrepancies generate legal uncertainty regarding what constitutes a 'sovereign' solution within the EU and accentuates market fragmentation. This is likely to slow down adoption of cloud-edge solutions by European organisations, particularly in sectors with stricter requirements, and further hamper the ability of EU businesses – providers and users – to achieve the economies of scale required to succeed in the data economy.

The report draws on the current context for the cloud-edge market, the unfolding regulatory debate on 'sovereign cloud', and the attitudes and priorities of European organisations relative to the topic of data sovereignty to inform the contours of three 'stylised scenarios' characterising future outcomes for the cloud-edge market:

- A ***"globalised free market"*** scenario tantamount to the situation in 2021 favouring self-regulation and laissez-faire leading to an uneven adoption of cloud-edge between industries as a function of the importance they attach to trust.

- A ***"fortress Europe"*** scenario wherein member states and the EU drastically limit the presence of non-EU cloud-edge providers and invest public funds to promote local solutions leading to different layers of regulation resulting in fragmentation.

- *An **"open strategic sovereignty"** scenario where the emphasis is not on excluding but rather on regulating service providers, through ambitious and harmonized data regulations and EU-wide industry-driven standards that promote trusted and competitive solutions.*

The economic analysis of these scenarios incorporates metrics such as trust, supply, adoption, market concentration and net value delivered to end-users. These data points are compiled from a combination of market data and survey responses from over 600 senior executives of EU-based public and private organisations, collected in May-June 2021 and in November 2021.

An important finding of this comparison is that the open strategic sovereignty scenario could deliver between 10-14 additional percentage points of cloud adoption across the continent by 2030 – 12 more points than the next best scenario – and generate up to 2.4 times more value from industrial data exchange and collaboration within and across sectors. Based on this analysis, the report puts forward concrete recommendations to achieve a strategically open approach to technological sovereignty in Europe, paving the way for European leadership in the development of cloud and edge services. These services will underpin the next generation of applications that will transform industries, making it paramount that Europe emerge as a leader in this space. While the cloud market is relatively mature, with established market leaders, the edge market is nascent with enormous potential. Europe's leadership in Industry 4.0 gives it a natural opportunity to be a leader in edge computing. Open strategic sovereignty is required for a thriving edge ecosystem and is therefore a key means to allow the EU to emerge as a leader in this field.

The evidence from the study points to a multi-faceted definition of sovereignty. Achieving open strategic sovereignty in the cloud-edge domain implies delivering trust – specifically through assurances in terms of compliance, cybersecurity, and transparency over location and accesses to data – together with measures that allow users to maximise the value of their data, through interoperability, portability, and ease of data sharing.

EU organisations express strong expectations regarding the latter when asked about the benefits they expected from "sovereign" cloud-edge solutions, notably due to the new value they seek to gain from cross-sector collaboration and data exchange. The study draws on actual edge-cloud solutions deployed by both Vodafone and other cloud-edge providers showcasing emerging technological solutions and ecosystems that seek to balance these new end-user requirements, with established demands in terms of quality and scope of service, as well as cost.

Furthermore, the facts depicted in the report indicate that the cloud market has evolved and that current levels of concentration, the low impact of voluntary codes of conduct, as well as emerging evidence of anti-competitive practices creates the case for more active regulatory intervention. More specifically, achieving open strategic sovereignty implies EU-level regulation and an industrial policy that seek to maximize the value generated from cloud-edge solutions through:

- ***Broad adoption of cloud-edge solutions*** across all types of sectors (from consumer goods to organisations critical to national security) by ensuring that the market addresses the market's diverse set of expectations in terms of ***trust, depth of services*** as well as ***total cost incurred by end users***

- ***A diverse supply of solutions*** consistent with Open Strategic Sovereignty, achieved through ***fair competition*** amongst cloud-edge providers and by ***regulating rather than excluding*** cloud-edge service providers from the EU market, to ensure that users can still benefit from investments in innovation made by firms who may not meet strict requirements for EU corporate 'control'.

- ***An environment that favours investment and innovation by technology providers,*** *enabled through* ***economies of scale*** *for all providers that make the effort to meet EU requirements thanks to* ***harmonised regulatory requirements within the EU,*** *as well as through support to private investments in innovative solutions, particularly in relation to multi-cloud and multi-edge interoperability.*

Striving to achieve this balance, the report proposes an action plan for policymakers built on five key recommendations detailed in the last chapter:

1. **Align on a harmonised definition of trusted cloud-edge services at EU-level that provides clarity to users and providers regarding the technical and operational requirements that must be met by cloud providers to be fully compliant with EU law.**

2. **Expedite the implementation of a pan-EU framework for cloud certification and a publicly accessible EU-wide 'registry' of EU-certified cloud-edge solutions.**

3. **Introduce fit-for-purpose regulatory oversight in the market for cloud-edge services to promote fair competition and fair distribution of value towards end-users across EU industries.**

4. **Strengthen existing EU regulation by adding obligations that favour a more competitive, transparent and innovative market, harmonised at EU level.**

5. **Promote investment in sovereign cloud-edge solutions in a manner consistent with abovementioned recommendations and that leverage "federated architecture" principles to meet users' data localisation requirements while maintaining free flow of data across approved jurisdictions.**

GLOSSARY

AI/ML	Artificial intelligence/Machine learning
API	Application programming interface
CaaS	Containers as a Service
CSP	Cloud Service Provider
EC	European Commission
ECJ	European Court of Justice
EEA	European Economic Area
EU	European Union
FFoDR	Free Flow of Non-Personal Data Regulation
GDPR	General Data Protection Regulation
GSMA	Global System for Mobile communications Association
IaaS	Infrastructure as a Service
IoT	Internet of Things
MEC	Multi-Access Edge Computing
MVNO	Mobile Virtual Network Operator
OS	Operating System
PaaS	Platform as a Service
SaaS	Software as a Service
SME	Small and medium-sized enterprises
SWIPO	Switching Cloud Providers and Porting Data

INTRODUCTION

As cloud and edge computing continues to proliferate, concerns relating to data sovereignty have gained prominence in Europe. Perceptions of sovereignty vary widely across policy spheres and industry. This report aims to analyse the current dynamics in the European cloud computing and edge computing market, particularly in regards to the way supply and demand are being impacted by the debate over European sovereignty and by the wider dynamics of the EU's industrial competitiveness, encompassing both the digital and green transitions.

Based on the insights drawn from two surveys of European public and private organisations, case studies and quantitative modelling of three scenarios, this study makes policy recommendations at EU and national level, as well as proposals to be considered by the cloud services and telecommunications industries[1].

The structure of the report is as follows:

- **Chapter 1** provides an overview of the market for cloud services in Europe, and the comparative benefits sought by end-users in established but also new emerging models, like edge computing

- **Chapter 2** sheds light on the current policy landscape, looking at the approaches to data sovereignty emerging at EU level, and Member State level, in the context of new proposed legislation and regulatory interventions

- **Chapter 3** deep dives into the attitudes and priorities of European organisations relative to the topic of data sovereignty, unpacking its implications from the point of view of different industries and detailing the different ways that users and providers are meeting evolving requirements in practice

- **Chapter 4** models and compares the outcomes of three policy scenarios, exploring how different regulatory and industry initiatives could influence the trajectories outlined in previous chapters

- **Chapter 5** outlines recommendations for policy and industry on how to achieve target outcomes, taking stock of findings from the abovementioned surveys and economic modelling.

[1] *Data is derived from two surveys conducted by Capgemini with senior executives from EU as well as non-EU private and public organisations, conducted in May-June 2021 and in November 2021. The first survey encompassed 610 respondents from EU countries as well as 390 respondents from Australia, India, UK, US for comparison on specific questions. The second survey focused on a subset of 251 respondents from 13 EU countries. Respondents stemmed from public and private organisations across all sectors, including SMEs with >50 m€ turnover. Public organisations represent 11% of respondents. A small number of survey responses led to follow-up interviews with respondents. Additional data and reference points are drawn from publicly available studies and resources referenced in the Appendix.*

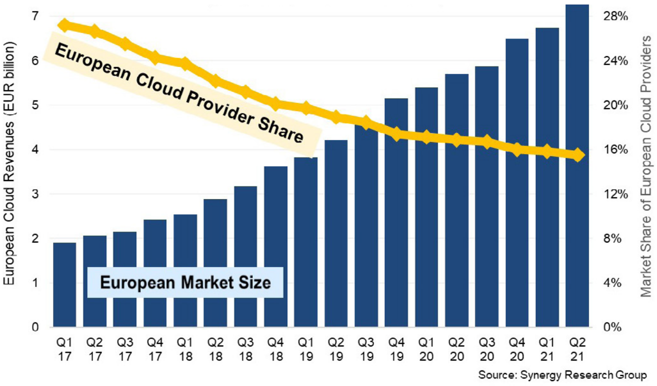
CHAPTER 1
OPPORTUNITIES FOR THE EU ECONOMY

The shifting market for cloud services

The COVID-19 pandemic has turbo-charged the adoption of cloud-based data solutions. In an unprecedented business environment, cloud services have proven crucial to remote-workforce collaboration and productivity, disaster recovery, cost control, agility, resilience, and business continuity. In fact, nine out of ten organizations increased their cloud usage in direct response to the pandemic[2]. The organisations that have most significantly adopted end-to-end cloud services stand out amongst peers in terms of growth, customer satisfaction and market capitalisation, regardless of the way their industry was affected by the crisis. After growing 18.4% in 2020, worldwide spending on Cloud Computing is forecast to grow by 25.9% in 2021[3].

Organizations across the public and private sector, large and small, local and global, are turning to cloud services both for the simplicity, flexibility as well as the innovative capacity it offers by delivering state of the art IT capabilities 'as-a-service' (see right). In Europe alone, the cloud market is expected to grow from €53bn in 2020 to €560bn by 2030[4]. Europe offers a particularly attractive opportunity in coming years due to relatively low levels of cloud adoption, particularly compared to North American markets[5]. This gap is expected to result to a high-growth catch-up phase, as seen in the Chinese market in recent years.

Cloud players have emerged on every continent over the years, but US-based providers have taken a leading position in every region. They have done so by being the first to leverage significant economies of scale, particularly in terms of capital expenditure for infrastructure services (known as Infrastructure-as-a-Service, or IaaS) and by gaining a first mover advantage in higher value developer services (known as Platform-as-a-Service, or PaaS). This is mostly true of three players – Amazon Web Services, Microsoft Azure, and Google Cloud Platform, referred to commonly as hyperscale cloud providers, or in short form, "hyperscalers" – who together accounted for 69% of the European cloud market in January 2021[6]. This share has consistently increased over the past decade despite significant growth in the market, underlining the difficulty faced by competitors to achieve similar economies of scale and catch up on service layers. The weight of these three 'generalist' US hyperscalers is supplemented by that of fast emerging smaller scale, often more specialised US-based providers like Cloudflare or Snowflake.



Source: Synergy Research Group

FIGURE 1: European Cloud Provider Share of Local Market (IaaS, PaaS, Hosted Private Cloud)

[2] Flexera, "2021 State of the Cloud Report", n=750, https://info.flexera.com/CM-REPORT-State-of-the-Cloud

[3] Gartner, "Forecast: Public Cloud Services, Worldwide, 2019-2025, 3Q21," September 2021.

[4] KPMG, "The European Cloud Market: key challenges for Europe and 5 scenarios with major impacts by 2027-30", April 2021

[5] Gartner, "Cloud Adoption: Where Does Your Country Rank?", 19 August 2019. EU cloud adoption statistics are updated annually by Eurostat – see https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Cloud_computing_-_statistics_on_the_use_by_enterprises

[6] Synergy Research, "European Cloud Providers Double in Size but Lose Market Share", September 2021, https://www.srgresearch.com/articles/european-cloud-providers-double-in-size-but-lose-market-share

FROM **CLOUD** TO **EDGE COMPUTING**

Cloud computing is best understood as a consumption model, rather than a technology. It enables as-a-service, i.e. 'pay as you go', consumption of a range of IT capabilities, from storage to compute and advanced analytics services.

Services can be delivered either via a public, private or hybrid cloud model. In the public model, capacities and costs are optimized by mutualising services across multiple organisations while keeping data segregated – a model known as multi-tenancy – while in the private model, an organisation can choose to conserve its own instance of cloud services on dedicated servers – 'single tenancy' - providing an extra layer of control and customization over services. The hybrid cloud model combines the advantages of both public and private cloud, by connecting a private on-premises datacentre with a public cloud, allowing data and applications to be shared between them.

Multi-tenancy and 'as a Service' models offer evident benefits in terms of cost, but also from an environmental perspective. The benefits of multi-tenancy and as-a-service delivery can be achieved at different scales and layers of the stack. Traditional 'centralised' cloud computing is run from a central data centre at often significant physical distance from the end user (>1000kms). These datacentres can be in different countries, and even different continents, to those of the users they serve. Centralised cloud technology emerged in the early 2000s and therefore these solutions have a higher level of maturity, resilience, and standardisation than other parts of the continuum. They are best suited for large amounts of data and higher-order computing. "Hyperscaler" providers like Microsoft Azure, Amazon Web Services and Google Cloud, as well as Alibaba and European players such as SAP; OVHcloud or Cloudferro all offer centralised cloud services.

Edge computing is a distributed cloud model that combines the benefits of as a service delivery, and if users choose, of multi-tenancy, with the benefits of decentralization. Processing and/or storage of data is done closer to where the data is produced or used, on the 'edge' of the core network – hence the term 'edge computing'.

These decentralized capacities vary in nature from on-premise data processing infrastructure (smart homes and factories) and servers located in points of concentration within cellular networks, all the way to on-device (IoT devices, mobile phones and connected vehicles). This leads to a distinction between different types of 'edges', depending on their proximity to the central cloud and core network: near edge, far edge, and on-device edge. Edge use cases are growing in commonality with the rise of 5G, which supports low latency.

This report uses the term cloud-edge to encompass this continuum and the range of solutions that fall within it including near edge and far edge.

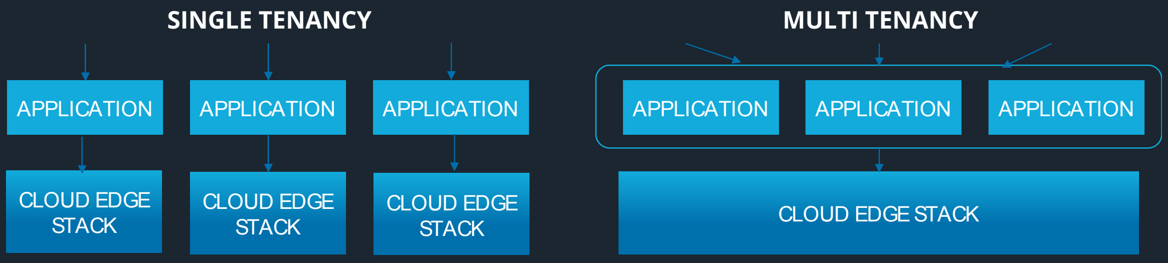


FIGURE 2: illustration of single-tenant and multi-tenant model

Why distributed cloud is not the same as going back to what existed before cloud computing

Solutions using edge computing can provide more than before cloud computing emerged, as they are able to utilise the centralised cloud as part of the offering. For example, installing a device on the motorway to capture the speed of cars was possible without cloud computing technology. However, performing analysis on that data requires infrastructure with capacity, this sort of infrastructure is expensive, cumbersome, and not appropriate to install every 10km on the motorway. Edge computing can relay the data to a common centralised cloud and back to the device enabling real time analysis at a fraction of the cost and effort. Advances in AI, machine learning and graphical processing power mean have high demands on computing resources, with a need for lower latencies – creating a need to bring compute closer to the end users to create highly immersive personalised application experiences.

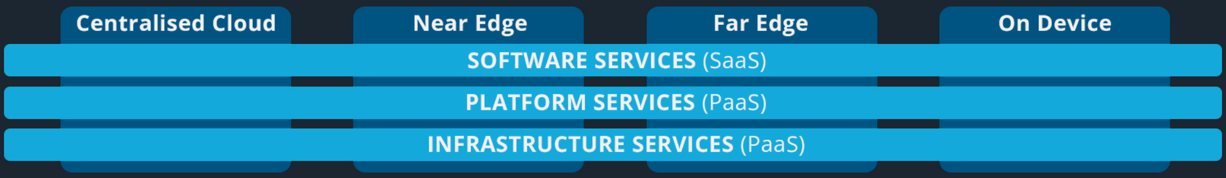


FIGURE 3: the cloud-edge computing continuum

EDGE COMPUTING: EUROPE'S CHANCE TO LEAD TOMORROW'S MARKET FOR INDUSTRIAL DATA AND DATA-RELATED SERVICES

While recent years have seen consistently increasing market concentration on the European (and global) cloud market, several new trends are at play today:

1. **The IaaS market has significantly matured in recent years, to the point where it is moving towards commoditisation, at least for 'centralised' cloud services. In practice, this means these types of services are becoming less of a source of innovation and differentiation between providers than other layers in cloud services[7].**

2. **The PaaS market is highly-prized, but only addressed by hyperscalers at this stage, and exclusively for centralised and near edge cloud capabilities.**

3. **Most development tools and cloud technologies are gradually moving towards standardisation and open access, reducing barriers to entry. This is particularly true for SaaS, which involves little capital expenditure for providers, but less so for IaaS and PaaS – capital expenditure remains high to entire the IaaS market, and the latter requires specialist skills that are in short supply.**

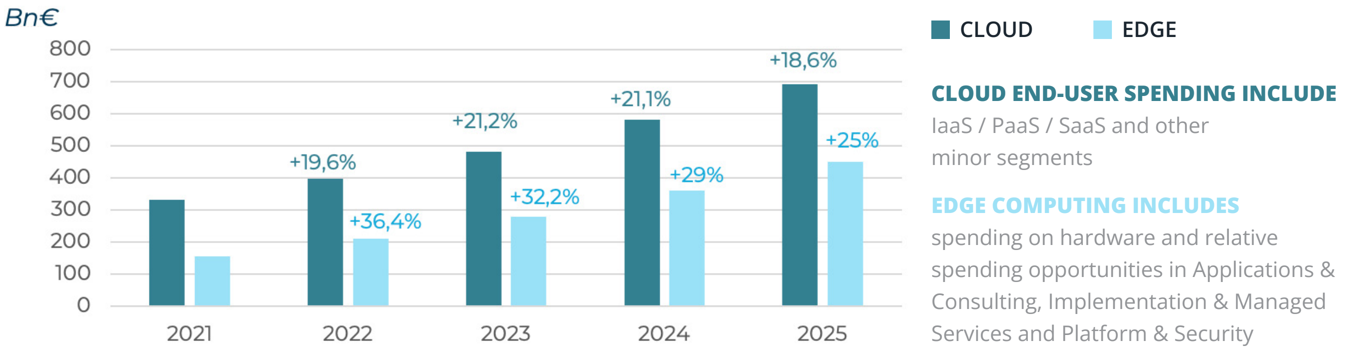
4. **New value is emerging from sharing and re-use of data across and between sectors. In fact, research conducted by the Capgemini Research Institute shows that organisations that leverage data sharing ecosystems are expected to generate between 2.4% and 9.4 % in additional cumulative revenue by 2030.**

5. **Meanwhile, the emergence of a decentralised 'edge computing' model opens a new market where economies of scales are expected to be lower, but synergies with other technologies (5G, IoT...) will be higher. The market for PaaS and SaaS services 'at the far edge', including MEC service platforms (see page 13 for an explanation of MEC) remains a blue ocean. Several players are eyeing all or part of this edge computing market: cloud providers, telecommunications operators, specialist edge data centre operators as well as IoT device manufacturers. The winners are likely to be ecosystems that manage to combine the expertise of these different players to overcome remaining R&D challenges in this field.**

The opportunity represented by edge computing is particularly significant. Overall, the growth of demand – globally and within Europe – is set to surpass that for centralized cloud across all types of services. This is primarily due to the fact it is expected to unlock untapped value from industrial data, hence benefit regions and industries with most advanced digitization of industrial processes.

What is "industrial data"?

Industrial data is a wide-ranging term that refers to any data generated by private and public organisations as a result of business processes, especially industrial processes. For instance, this can be data produced by enterprise management systems, operating data of a machine in a manufacturing plant, or performance logs generated by an autonomous vehicle. Industrial data primarily consists of non-personal data, by contrast to consumer data, and is significantly less standardised than consumer data, requiring deep understanding of industrial processes and ability to handle proprietary formats from different equipment manufacturers.



CLOUD END-USER SPENDING INCLUDE
IaaS / PaaS / SaaS and other minor segments

EDGE COMPUTING INCLUDES
spending on hardware and relative spending opportunities in Applications & Consulting, Implementation & Managed Services and Platform & Security

***FIGURE 4:** Global forecast of end-user spending on cloud vs edge computing and key factors expected by industry from cloud (IaaS, PaaS, Hosted Private Cloud)* [8]

[7] *However, as explored in Chapter 2, this has not resulted in direct price competition between players, due to the particularities of current competitive dynamics in the cloud market.*

[8] *Gartner - Forecast: Public Cloud Services, Worldwide, 2019-2025, 1Q21 Update / Leading the Edge: Gartner's Initial Edge Hardware Infrastructure Forecast*

Interestingly, edge computing is also primarily perceived by industry as a way of meeting their requirements in terms of data security and compliance, which as shown later in this report are a key concern for industry at large, but even more so for European players. This is due to the fact edge computing allows for greater direct proximity and control over data and applications, allowing users to process sensitive data on-premise and send non-sensitive elements – including aggregated algorithm results or pseudonymized data sets – to central cloud infrastructure.

Edge computing deployments will also natively combine different types of technologies including 5G, IoT, together with industry-specific machinery and processes. The most mature deployments demonstrate that this is best achieved by projects that are able to leverage an ecosystem of edge operators, connectivity providers, and industry users to meet requirements for use cases. This is especially true for Multi-Access Edge Computing (MEC).

Finally, the specificities and technological diversity involved in edge computing will lead to higher volumes of system integration and custom software development, a domain where European industry performs well in terms of skills and size, within the EU and on a global level.

Together, these factors make edge a significant opportunity for European industry to introduce greater competition into the market and unlock new types of value from industrial data, in the interests of end users.

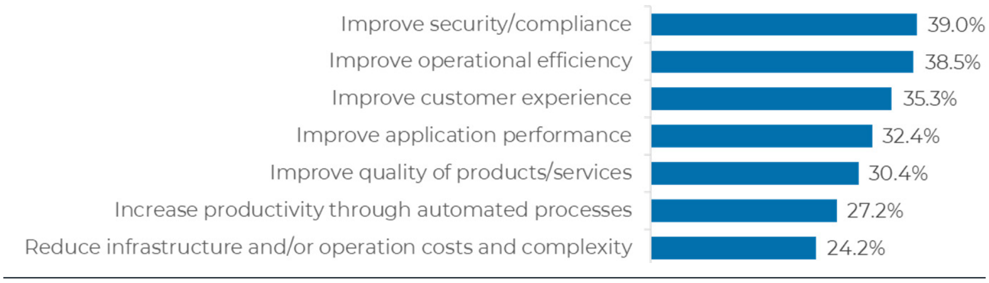


FIGURE 5: Benefits expected from edge computing by organisations (global) [9]

MEC MULTI-ACCESS EDGE COMPUTING

Multi-access edge computing (MEC) offers cloud computing capability at the furthest edge of a network. Previously known as mobile edge computing, MEC bridges the gap between connected devices and the cloud and is truly game-changing in situations where milliseconds matter. By moving some of the computing capability out of the cloud and closer to the end user and devices, data does not have to travel. This leads to greater performance, dramatically reduced latency, contextually aware applications, reduced carbon footprint and improved security.

MEC technology is widely used in video analytics, location services, augmented reality, local content distribution and is expected to play a key role in enabling the use of autonomous vehicles. Its success crucially depends on a strong collaboration between telecommunications operators, cloud service provider and IoT equipment manufacturers to ensure the necessary levels of interoperability.

Vodafone's MEC solution with AWS Wavelength has been used cross-industry for its ability to quickly experiment a range of use cases. In each instance, end-users have worked with Vodafone to meet the data security and compliance requirements necessary to experiment on sensitive data. For example, HERE Technologies have coupled their location platform, which predicts hazards on the road and warns drivers before anything has even happened, with distributed edge computing to trial a real-time warning system with Porsche. Italy's state-owned rail company, Ferrovie dello Stato Italiane, has been experimenting Vodafone's MEC to trial an innovative surveillance solution for real time insights on the happenings in one of their historic train stations.

With its customers and partners, Vodafone has developed both dedicated and distributed MEC solutions. Dedicated MEC is deployed at a customer's site on a mobile private network and is dedicated to one organisation. The other variant, distributed MEC, runs on a public 4G/5G network and is used especially when connecting moving nomadic assets.

Network architecture standards for MEC are governed by the European Telecommunications Standards Institute (ETSI). For more information, see: https://www.etsi.org/technologies/multi-access-edge-computing

[9] *IDC Edge Computing Solutions Powering the 4th Industrial Revolution, January 2021*

CHAPTER 2
POLICY CONTEXT AT EU AND NATIONAL LEVEL: THE SOVEREIGNTY DEBATE

As set out in the previous chapter, cloud computing has taken a central role in both digital transformation of organisations and ability to derive value from data. The value and benefits of cloud computing technology are also extending beyond the traditional sphere of IT, and moving into the physical world with edge computing: from connected vehicles and hand-held devices to industrial machines and processes.

The increasingly ubiquitous nature of cloud-based technology, together with the fact that leading cloud providers now rank as the top global companies by market capitalisation has made it a key topic for policymakers in recent years, in terms of data protection and cybersecurity policy but also in terms of economic policy and industrial strategy. This is particularly true in Europe, where policymakers have shown growing concern with the low levels of cloud adoption across Europe compared to US and several Asian markets, and the fact that all leading global cloud service providers – but also fast emerging smaller scale providers – are predominantly based outside of the continent.

The present chapter reviews the key policy debates as well as existing and proposed requirements brought forward by regulators across Europe. The chapter first looks at policies implemented and proposed at EU level. This is followed by an analysis of national-level cloud policies in four Member States currently most active in this field.

THE LIMITS OF SELF-REGULATION FOR PORTABILITY

The GDPR and FFoDR encourage the development of self-regulatory codes of conduct that serve to detail best practices and help providers achieve compliance with regulatory obligations. Two such examples are the codes of conduct – one for IaaS services, the second for SaaS services – proposed by the working group on Switching Cloud Providers and Porting Data to facilitate the proper application of the FFoDR's Article 6 requirements on porting of data (hence known as the SWIPO codes of conduct)[10]. The codes establish a set of requirements that seek to enable safe migration of data and services between cloud service providers as well as between a provider and users' own (on-premise) infrastructure and/or applications. Under the code, providers are also required to ensure sufficient transparency such that users can easily assess the level of effort required to achieve portability when choosing their solution.

In practice, these codes have been criticised for their limited impact, primarily due to their voluntary nature. The SWIPO code relating to SaaS services has also been criticised for more readily accounting for the views of large global providers to the detriment of users and small providers[11].

The European Commission will evaluate the impact of those Codes of Conduct before November 2022. This evaluation will notably focus on the effects that the SWIPO Codes of Conduct have had on the fluidity and competitiveness of the cloud market. The limited impacts observed to date are expected to result in stricter regulations, with the Commission publishing hard legal requirements for cloud service providers to ensure portability as part of the EU Data Act published in February 2022.

[10] *Available here: https://swipo.eu/wp-content/uploads/2020/10/SWIPO-IaaS-Code-of-Conduct-version-2020-27-May-2020-v3.0.pdf https://swipo.eu/wp-content/uploads/2020/07/SWIPO-SaaS-Code-of-Conduct.pdf*

[11] *See for example comment shard by the Cigref, an association of large businesses and public administrations in France: https://www.cigref.fr/swipo-failure-regulate-european-cloud-market*

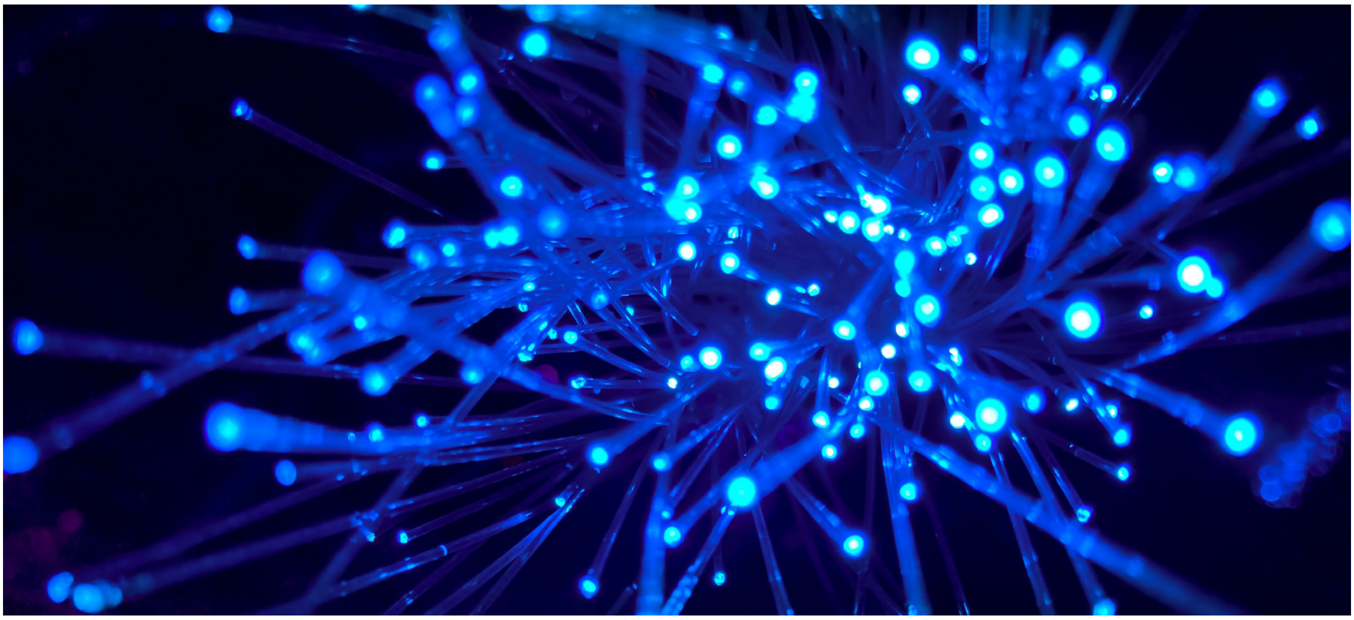
THE VIEW FROM BRUSSELS: SEEKING LEADERSHIP IN INDUSTRIAL DATA

In the past decade, European policymakers have enacted the building blocks of a 'single market for data' at EU level. However, there is potential for more significant intervention in response to increasing concerns that insufficient or unfair competition in the market for data, cloud and edge services is resulting in poor outcomes for EU-based users and providers of such services.

To date, two key pieces of EU regulation have shaped the data economy, both within and beyond the borders of the European Union. The General Data Protection Regulation (GDPR) was the first to come into force: originally proposed in January 2012, adopted by European institutions in April 2016, the GDPR has been applicable to all entities that process the data of EU citizens since 25 May 2018, and is widely perceived to have transformed the way organisations handle and protect personal data around the globe. It was supplemented in December 2018 by the Free Flow on Non-Personal Data Regulation (FFoDR), effective since May 2019. While they impose stricter requirements on the handling personal data, together, these two regulations create a harmonized legal framework that guarantees free movement of data (personal and non-personal) across the EEA as well as with a limited number countries whose data protection regimes are formally considered adequate by the European Commission[12]. The list includes Switzerland, New Zealand, Japan, as well as the United Kingdom[13], for which the Commission found that data protection guarantees are such that they also enable data exchange for law enforcement purposes[14].

Yet, a series of factors are causing the current Commission to plan further intervention.

First, while the impacts of GDPR on the way organisations handle and protect personal data have been felt around the globe, the EU's attempts to promote interoperability and portability of data and applications has been more limited, to date stopping short of binding legal requirements for cloud service providers in favour of co-regulatory measures to promote and facilitate data portability and switching. The potential of the GPDR's and FFoDR's portability requirements to enable novel data flows and foster competition is recognised in reports for the Commission and Member State governments, as well as beyond the EU[15]. Yet, their reliance on voluntary codes of conduct has proven relatively ineffective, demonstrating the limits of self-regulation (see insert). Moreover, as a result of being designed to promote switching of service providers rather than sharing and re-use of data and services between organisations, the regulations' portability and interoperability requirements have not led to the much hoped-for generation of new value from "data ecosystems".



[12] *Following Article 1(3) of the GDPR, organisations and Member States cannot restrict the free movement of personal data within the EU, unless justified under one of the allowed exemptions (e.g. for national security or law enforcement purposes). Article 4(1) of the FFoDR only permits restrictions on the free flow of personal data based on public security.*

[13] *In total, 14 jurisdictions have been recognized as providing an adequate level of protection under GDPR by EU institutions: Andorra, Argentina, Canada (commercial organisations only), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland , the United Kingdom, and Uruguay https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en*

[14] *The EC adopted this adequacy decision on 28 June 2021, having assessed that "UK's data protection system continues to be based on the same rules that were applicable when the UK was a Member State of the EU". The UK is the only country for which the EC's adequacy decision also covers data exchanges in the law enforcement sector under the EU Law Enforcement Directive. https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3183*

[15] *J. Cremer, Y-A deMontjoye and H. Schweitzer, Competition policy for the digital era, May 2019. Digital Competition Expert Panel, Unlocking digital competition, report for the UK government, March 2019. See as well the introduction of a new Consumer Data Right in Australia, https://www.accc.gov.au/focus-areas/consumer-data-right-cdr-0 and the consultation in on data portability in Singapore.*

Second, European policymakers, competition experts and industry have expressed strong concerns regarding alleged unfair competitive dynamics allowing a handful of established players to strengthen or cement their market share. A recent study led by Professor Frédéric Jenny, Chairman of the OECD's Competition Committee and formerly Vice Chair of France's Competition Authority, documents a series of technical, financial and contractual practices observed in the SaaS market which it alleges are employed to "lock-in" business users within established software providers' own cloud infrastructure. The practices identified in the study include:

- De facto higher prices for enterprise software purchased for use on third-party cloud infrastructure.
- Bundling or tying SaaS & IaaS services in such a way that the low (possibly anti-competitive) cost achieved on part of the bundle might rule out other cloud infrastructure providers from being competitive, and in any case lessen users' ability to compare offers with alternative providers.
- Limiting data portability – technically, or by charging "egress fees" – to make it costly if not impossible to use alternative cloud infrastructure
- Limiting or removing the option to "Bring Your Own Licence (BYOL)" meaning customers are forced to pay again to use software they already own on competing cloud infrastructure.
- Demanding customer information from partners for billing purposes but then approaching those customers directly to solicit them to switch cloud infrastructure.

If left unchecked, the study suggests, these unfair practices will damage growth, innovation and viability of alternative data infrastructure and platform providers (IaaS and PaaS), and ultimately lead to less choice and higher prices for consumers. Such practices strengthen the view that the economic characteristics of cloud computing – significant first-mover advantage and barriers to entry, due to high initial investments and continuously decreasing marginal costs – grant established cloud infrastructure (IaaS) and platform (PaaS) providers a 'gatekeeper' status. Similar allegations had already come to the fore in an investigation published in 2020 by the US' House of Representatives Judiciary Committee[16]. It is also worth noting that on 28 January 2022 the French competition authority announced it was initiating proceedings ex officio to analyse competition conditions in the cloud computing sector.[17]

Third, policymakers and industry have also expressed concerns that use of non-EU-based cloud service providers could expose users to extra-territorial legislation incompatible with EU law, notably US and Chinese laws relating to data access for law enforcement and national security purposes. These concerns have come to the fore in a case called Schrems II, where an EU citizen argued that the EU-US Privacy Shield was not, in fact, adequately safeguarding data under the GDPR due to provisions in the US Foreign Intelligence Surveillance Act[18]. The resulting decision by the ECJ, invalidating the Privacy Shield, has created significant legal uncertainty and brought discussions on choice of cloud providers up to the boardroom of EU organisations.

Fourth and last, the above concerns are compounded by the enduringly low levels of cloud adoption observed across the Europe and the relatively small footprint of European players in the global data economy, as evidenced in Chapter 1.

The appointment of the von der Leyen Commission brought in new impetus and its refreshed EU Data Strategy, published in February 2020, takes stock of the above cited concerns on lack of competition, adoption and data sovereignty. Announcing the strategy, EU Commissioner Thierry Breton laid out the EC's view that while Europe may have "missed the battle for personal data" – specifically, the battle for economic value of personal data – to predominantly US and Asia-based businesses, today's market leaders will not necessarily be tomorrow's leaders, due to the significantly wider and more complex opportunities offered by industrial data for which the commissioner expects "Europe |to] be the main battlefield"[19]. The EU data strategy seeks to capture these opportunities.

To that effect, the EC has set out plans for a much more far-reaching set of interventions in the market for data, cloud and edge computing services. On one hand, it plans to enact several new pieces of regulation – a Data Governance Act, a Data Act and a Digital Markets Act – by 2024. Together, these legislative instruments are expected to go far beyond existing regulations and codes of conduct, notably by mandating data portability and interoperability as well as requiring the creation of independent third parties to play the role of 'data intermediaries', thus preventing cloud providers from indirectly profiting from the data they store for clients. An EU-wide cybersecurity certification for cloud services is expected to complete these legislative requirement[20]. Developed by the European cybersecurity agency (ENISA), following the framework laid down in the Cybersecurity Act, European certification schemes will start out as voluntary schemes, with an option to make them mandatory after assessing its effectiveness.

[16] Investigation of competition in digital markets, Majority staff report and recommendations of the US House Judiciary Subcommittee on antitrust, commercial and administrative law, October 2020

[17] The investigation will examine the competitive dynamics of the sector and the presence of players in the various segments of the value chain, as well as their contractual relationships, in an environment in which multiple alliances and partnerships are concluded for the provision of cloud services. The Autorité de la concurrence may, where appropriate, make proposals to improve the competitive functioning of the sector. https://www.autoritedelaconcurrence.fr/en/press-release/autorite-de-la-concurrence-starts-proceedings-ex-officio-analyse-competition

[18] Section 702 of FISA requires cloud providers to supply U.S. intelligence agencies with the data they manage, as well as the encryption keys to decrypt that data, relating to non-U.S. persons identified by the agencies. Though it was not considered in the ECJ's decision, similar concerns have been raised concerning the CLOUD Act, which allows US courts to issue a search warrant compelling US cloud providers to provide all data of an individual, without seeking authorization from the courts of the country where the individual or the data are located (even if the data is hosted outside the US, e.g. in the EU).

[19] See https://ec.europa.eu/commission/presscorner/detail/en/READ_20_377 Limited ability to catch up to US and Chinese giants when it comes to services built on personal data. Industrial data offers more potential, for the same reasons that makes edge computing high potential as cited in previous chapter

[20] See: https://www.enisa.europa.eu/news/enisa-news/cloud-certification-scheme

All regulatory requirements and sector-specific guidance for cloud providers wishing to deliver services within the EU will be consolidated into an “EU Cloud Rulebook”. This Rulebook aims to give providers a ‘one-stop-shop’ compilation of regulatory as well as industry-driven cloud certifications and codes of conduct along with coherent guidelines on how to comply with EU cloud market rules cloud providers. The EU data strategy also reveals plans to setup a European cloud services marketplace that aims to level the playing field between new or small cloud service providers and incumbents and strengthen overall compliance of providers with EU requirements. It is expected to do so by indicating the level of compliance of a given cloud service with regulatory requirements and industry standards, notably those that make up the EU Cloud Rulebook, as well as by improving users’ ability to compare services of different providers.

Lastly, as part of its wider Industrial Strategy, the EC and Member States have committed to investing over 8 billion euros[21] in the development of data, cloud and edge computing services that meet its requirements. The EC expects this to be matched by private sector investments, in particular via a dedicated IPCEI (Important Project of Common European Interest) through which European firms are incentivised to collectively invest in innovative cloud-edge solutions for the European market, co-funded by Member States. In December 2021, the EC launched the Alliance on Industrial Data, Edge and Cloud, a body composed of policymakers and industry representatives that aims to help plan the capacities and public-private investments required to achieve the Commission’s Digital Decade targets for 2030.

LESSONS LEARNED FROM THE TELECOMMUNICATIONS INDUSTRY: A TEMPLATE FOR REGULATION IN THE CLOUD-EDGE DOMAIN?

Lessons learned from regulatory interventions in the telecommunications sector offer a fitting template for European policy in regard to cloud and edge computing.

EU-level regulatory interventions in the telecommunications domain have driven improvements competition and choice for end-users. Regulatory switching obligations facilitate competition in telecoms markets, notably by enabling consumers and businesses to easily switch providers and port numbers.

The mechanics of how the switching process should work is subject to intense regulatory scrutiny, and has matured over the last 20 years. Policy has shifted from a ‘losing provider’ led process (where the incumbent has every opportunity to frustrate or delay the switch) to a ‘gaining provider’ led process (where the new provider has more control over the switching process).

Timescales for switching have reduced considerably from weeks, to days and most recently, hours. A greater variety of sanctions have been introduced to drive compliance, with the European Electronic Communications Code specifying that Member States lay down rules on the compensation of end-users in the case of failure of a provider to comply in the case of delays in, or abuses of, porting and switching process. The technology has also evolved as the service portfolio has evolved – with ‘over the air’ switching being pioneered (and deployed) in relation to Internet of Things devices - for example an installed base of cars which are to be switched from one provider to another. This has been driven by the GSMA.

By way of further context, in the mobile market, there are now a number of different players driven by regulatory intervention in the market and continuing market innovations. Before competition was fully achieved in the retail market for mobile services, there was a regulatory obligation (as part of EU telecoms regulation) on mobile operators to provide wholesale access to MVNOs. This condition was introduced on the basis of a competition assessment in the relevant market and withdrawn when the market was deemed to be competitive. With 5G, a new model has emerged, known as the ‘neutral host provider’ model. The Neutral Host model is a technology solution that is agnostic in terms of which mobile network operator it supports, to cover the needs of various stakeholders in rural and poorly served areas. A number of mobile operators have pursued this model in order to promote the breadth of service offerings it the market.

In the context of telecommunications, it is now standard practice that end-users are able to switch connectivity providers in order to drive consumer choice and promote competition in the market. In the current cloud-edge market, hyperscaler cloud providers have gained a significant ability to influence market outcomes, due to their alleged “gatekeeper” status.

Although there are differences, at a high level a comparison can be made with the early days of the mobile telecoms market, and today’s cloud market.

Realising the full value of industrial data requires a shift away from this paradigm. For example, low latency, mobile scenarios will require that users have plug onto the closest cloud-edge infrastructure, irrespective of its provider. Users will need a service that moves their data with them across the network. EU policy requirements must go beyond existing voluntary industry codes of conduct to achieve this level of portability.

[21] 2 bn€ will come from EU budget, while 6 bn€ is expected to come from Member States, via the European Recovery & Resilience Fund.

EMERGING REGULATORY APPROACHES AT **MEMBER STATE LEVEL**

Concerns regarding the current competitive dynamics in the cloud market, limited adoption levels in public and critical infrastructure sectors, and perceived risks of exposure to extra-territorial legislation have also made a strong – sometimes stronger – mark at national level. Over the past 12 months, several EU Member States have stepped ahead of Brussels and either enacted or planned to enact policies governing the use of cloud-edge services within their borders. This section provides a comparative view of such policies in four countries: France, Germany, Italy and Spain.

These policies generally distinguish three 'levels' of requirements, based on the entities to which they apply: public organisations; critical infrastructure and service providers; and the economy at large (i.e. organisations that do not fall within either category). While the precise scope of sectors and entities that are within the realm of "critical infrastructure and services" varies from country to country, the term refers to organisations whose operations are essential to the functioning of a society and economy, and who must thereby abide by strict security (including cybersecurity) and resilience requirements. This typically encompasses major players in sectors like energy and water distribution, telecommunications, financial services, public health, transportation and national security.

Requirements	France	Germany	Italy	Spain
🟥 Government-specific cloud offers	Public institutions have the option to use government operated clouds (two in existence)	A cloud for public administrations is planned to be developed	A cloud for public administrations is planned to be developed	A cloud for public administrations is planned to be developed
🟥 'Cloud first' policy	Cloud must be used for all new uses unless justified otherwise	Expected to be required or strongly incentivised		
🟥 Multicloud portability	Portability is required	Expected to be required or strongly incentivised		
🟥 Application and data reversibility	Reversibility is required	*Not specified to date*		
🟥 Compliance with GAIA-X interoperability principles	Strongly incentivised	Expected to be required or strongly incentivised		
🟥 Publication of source code	*Not specified to date*	Expected to be required if using private cloud solutions	*Not specified to date*	Implied within plan for transparency policies
🟦🟥 National Cybersecurity Certification	Providers must be compliant with ANSSI SecNumCloud Certification	Providers must be compliant with BSI C5 Certification	An ACN 'Qualified Cloud' certification is planned	Currently applicable to public sector, the ENS applies to cloud and non-cloud services
🟦🟥 Immunity from non-EU legislation	Required for all "sensitive data"	Requirement expected to emerge		*Not specified to date*
⬜🟦🟥 Compliance with EU Data law	Harmonised requirements across all Member States stemming from GDPR and FFoDR			
⬜🟦🟥 Compliance with sector-specific regulatory requirements	Patchwork of EU-level and national requirements depending on each sector			

🟥 Impacts Public Sector 🟦 Impacts critical infrastructure ⬜ Impacts rest of industry

FIGURE 6: *Overview of EU country data policy requirements*

1. REQUIREMENTS FOR PUBLIC-SECTOR ORGANISATIONS

FRANCE

In 2021, France published two key documents that update the doctrine for use of cloud by public entities: the 'Cloud au centre' doctrine[22] (17 May 2021) and ministerial circular n° 6282-SG[23] (5 July 2021). These documents set out the following requirements for public organisations, based on a discussion between "cloud services for developers" (encompassing IaaS/PaaS) and "cloud services for end-users" (SaaS).

"Cloud au centre" can generally be translated by "Cloud first" and signifies a change whereby the use of cloud-based services becomes the default requirement for all new digital projects launched by public sector entities. Exceptions from this rule must be justified by providing a comparative analysis of the economic, legal, business and cybersecurity advantages of their solution relative to a cloud-based solution (e.g demonstrating that their solution offers lower maintenance costs or better meets the business need without compromising on security and legal risks).

Public organisations either have the option to use one of two government-operated clouds (generally reserved for classified data and only offering basic IaaS services) or to use a commercially available solution. Commercially available cloud solutions procured by public entities must ensure compliance with GDPR (and where applicable, sector specific labels like HDS for health data), multi-cloud portability[24], as well as application and data reversibility. The doctrine also strongly encourages compliance with Gaia-X interoperability principles[25].

But most importantly, these documents set out that for applications that handle "sensitive data" (defined very broadly as personal data of French citizens and business applications used by public servants but also economically sensitive industrial data), public organisations must ensure that cloud solutions be both compliant with the existing national cybersecurity agency's SecNumCloud certification and "immune from non-EU legislation"[26]. France's national cybersecurity agency has detailed this requirement as requiring cloud solutions to be commercialized by EU-headquartered entities, with a majority of EU-based share ownership and ensuring data to be stored and processed exclusively in EU countries[27].

Cloud services that meet these two requirements (compliance with SecNumCloud and immunity from non-EU law) will be certified as 'Cloud de Confiance', or 'Trusted cloud'. It is worth noting that even in cases where data is not considered sensitive, public organisations remain encouraged to use services that are certified as 'Cloud de Confiance'. The doctrine currently grants public organisations exemptions from 'Cloud de Confiance' compliance as no commercial solutions are yet certified, but this exemption will end 12 months after the first commercial solution becomes certified.

GERMANY

In Germany, no equivalent public documents exist at the time of writing, but a similar doctrine is expected to be published in 2022 in regards to public sector's use of cloud. The coalition agreement[28] published by the incoming administration on 24 November 2021 specifically plans for:

- A multi-cloud strategy including the development of a specific "cloud for public administrations" (this could be tasked to commercial providers) with "strict security and transparency requirements and open interfaces".
- Public sector IT projects to use open source and open standards, and for the "source code to be made public".

In the absence of clear guidance on the use of cloud, the public sector has tended to avoid public cloud services and focused on private cloud. Still, it is understood that the German government seeks to build a sovereign cloud solution that meets specific national requirements, continuing on from the plans of the previous administration. This is expected to be operated by a national technology leader.

Finally, it is worth noting that Gaia-X emerged through direct involvement of the German Ministry of Economy (BMWi) and that the government will likely seek to champion the standards that come out of the initiative[29].

[22] *Available here: https://www.numerique.gouv.fr/espace-presse/le-gouvernement-annonce-sa-strategie-nationale-pour-le-cloud*

[23] *Available here: https://www.legifrance.gouv.fr/download/pdf/circ?id=45205*

[24] *Alternatively, public entities must prove that the savings of not doing so are higher than the cost of porting the data.*

[25] *See chapter 3 for more detail on Gaia-X.*

[26] *For reference to the principle of immunity from non-EU regulation, see rule R9 of ministerial circular n° 6282-SG (5 July 2021). It is also cited here, inas well as a public letter from the Chief Digital Officer of France's civil service, dated 15 September 2021: https://acteurspublics.fr/upload/media/default/0001/36/acf32455f9b92bab52878ee1c8d83882684df1cc.pdf*

[27] *See the ANSSI proposed updates to the SecNumCloud requirements, page 53: https://www.ssi.gouv.fr/uploads/2021/10/anssi-referentiel_exigences-secnumcloud-v3.2.a_revision.pdf*

[28] *https://www.spd.de/fileadmin/Dokumente/Koalitionsvertrag/Koalitionsvertrag_2021-2025.pdf*

[28] *Available here: https://www.spd.de/fileadmin/Dokumente/Koalitionsvertrag/Koalitionsvertrag_2021-2025.pdf*

[29] *See chapter 3 for more detail on Gaia-X.*

ITALY

Italy published its first national cloud strategy[30] on 7 September 2021. Branded as "Cloud First" in its official translation, it positions the cloud as a priority for digital transformation of public administrations while setting out strict requirements. The strategy is based on three pillars.

First, the creation of the National Strategic Hub (NSH), "a national infrastructure for the provision of Cloud services, whose management and control are independent from non-EU providers". A public call for proposals was launched in September 2021, and on 27 December 2021, the Italian government announced it had selected the technical proposal jointly submitted by TIM-Leonardo-CDP-Sogei to serve as a blueprint for its upcoming 2 billion euro public tender to develop the NSH, due to be launched in 2022[31]. While respondents to the call for proposals decided to set aside partnerships with US-based players like AWS, Microsoft or Google in this first phase, officials have said that these organisations could provide their technology to the national cloud hub if it is licensed to companies selected to take part in the NSH project.[32]

Second, the introduction of a "qualification process of public Cloud providers" and their services to ensure that their characteristics and service levels are in line with the necessary requirements of security, reliability and compliance with relevant regulations and the country's national interests. This is expected to be similar to Germany's C5 certification and France's SecNumCloud certification. A national cybersecurity agency ('ACN') is being created for this purpose as part of a wider strategy and work program, but it is far from the level of maturity of its German and French equivalents.

Third, the development of a methodology for the classification of data and services managed by public administrations to allow their migration towards the most appropriate Cloud solution (NSH or qualified public Cloud). This methodology sets outs which types of data require data localization in Italy, data localization in EU, or no specific localization requirements (see page 11 of the strategy). Other requirements set out in the strategy are similar to those set out in France's 'Cloud de Confiance' doctrine, though less specific at this stage. For example, in relation to the topic of "immunity from non-EU regulation", the Italian doctrine emphasises the provision of "services, whose management and control are independent from non-EU providers"[33].

SPAIN

The Spain Esquema Nacional de Seguridad (ENS) security framework was established as part of Royal Decree as far back as i 2010. Public data assets must be classified under the ENS security levels (low, intermediate, high) to determine the security controls and frameworks required to protect the data adequately[34]. The ENS security approach applies to both cloud and non-cloud services. CSPs are therefore able to service the public sector if they are certified to the appropriate level to handle the sensitivity of the data and must be audited regularly to maintain their level of certification.

Spain has set obligations on public administrators to connect their information systems using a government-operated network called SARA[35], which is the cornerstone of the new Spanish Public Administration Cloud[36], due to be delivered as part of Spain's 2021-2025 Digitalization Plan for Public Administrations. The plan describes a hybrid cloud solution, which will house data from different ministerial departments in mutually public and private data centres across that deliver capabilities as-a-service. These activities are expected in line with cloud infrastructure initiatives at the European level, implying that solutioning will be in alignment with EC guidance. Additionally planned are transparency policies, encouraging open data management and exchange. The State Secretariat for Digitalization and Artificial Intelligence (SEDIA) has also expressed support for the interoperability principles being developed by Gaia-X.

[30] *https://innovazione.gov.it/notizie/articoli/en/the-italian-cloud-strategy*

[31] *https://innovazione.gov.it/notizie/articoli/cloud-pa-selezionato-il-progetto-psn-gara-prevista-nelle-prossime-settimane*

[32] *https://www.reuters.com/article/italy-cloud/update-2-italy-to-award-tender-for-national-cloud-hub-by-end-2022-idINL8N2Q93K7*

[33] *https://assets.innovazione.gov.it/1634299767-strategiaclouden.pdf*

[34] *https://www.enisa.europa.eu/publications/security-framework-for-govenmental-clouds/annex-a-b-case-studies-and-interviews*

[35] *https://administracionelectronica.gob.es/pae_Home/dam/jcr:c709e2ca-488d-4761-a8a7-f7e34dea1d23/SARA_EN.pdf*

[36] *https://joinup.ec.europa.eu/collection/egovernment/news/spanish-government-approv*

2. CRITICAL INFRASTRUCTURE AND SERVICE PROVIDERS

FRANCE

Critical infrastructure and service providers (healthcare, telco, energy, mobility providers, as well as part of aerospace-defense industry) must ensure that their systems are compliant with the ANSSI's (French national cybersecurity agency) SecNumCloud certification. Take-up has been slow, and availability of certified services remains very limited – only a handful of very basic IaaS and SaaS services[37], though several more are awaiting certification. The requirement of immunity from non-EU law applies to all critical infrastructure providers who currently fall under its scope.

GERMANY

Similarly, German critical infrastructure providers must ensure their cloud services are compliant with the BSI's (German federal cybersecurity agency) C5 certification[38]. This certification has similar requirements to the ANSSI SecNumCloud certification.

ITALY

Similarly, Italian critical infrastructure providers will need to ensure their cloud services are compliant with the forthcoming ACN's 'Qualified cloud' cybersecurity certification, but the requirements are still being defined. As stated above, they are likely to be similar to BSI C5 and ANSSI SecNumCloud. The requirements are expected to be enshrined into law by an executive act implementing the national "Law on cybersecurity perimeter", expected in July 2022. The law is however expected to increase the number of notifications required from providers to the government, and result in more lengthy approval processes.

3. ECONOMY AT LARGE

No country-specific requirements exist regarding the use of cloud by entities that fall outside the two previous categories. However, the ECJ's Schrems II decision, invalidating the Privacy Shield, has created legal uncertainty regarding the use of US-based cloud providers by EU businesses. Some private businesses have expressed concern with existing providers and interest in the certifications being developed by governments, though this remains a minority-held view. Once adopted, the GAIA-X compliance & labelling framework (described below) may fill a gap for these players and steer demand towards 'GAIA-X compliant' cloud solutions.

Overall, despite concerns, industrial users remain limited by the lack of maturity of European cloud offerings (IaaS or at best CaaS). Experts interviewed in each country indicate that instead of shifting completely away from US-based providers, the current dynamic is pushing industrial users towards a more multi-cloud strategy. This is particularly true in Germany.

[37] *The list of qualified providers, regularly updated by ANSSI, is available here: https://www.ssi.gouv.fr/entreprise/qualifications/prestataires-de-services-de-confiance-qualifies/prestataires-de-service-dinformatique-en-nuage-secnumcloud*

[38] *Available here: https://www.bsi.bund.de/EN/Topics/CloudComputing/Compliance_Criteria_Catalogue/Compliance_Criteria_Catalogue_node.html*

WHAT THIS MEANS FOR FUTURE CLOUD MARKET IN **EUROPE**

European policymakers and industry have entered a key phase – decisions taken in the coming 12-24 months will have a significant impact on Europe's future position in the global data economy, and on outcomes for EU-based users, from public institutions to industry.

The cloud market has evolved and current levels of concentration, low impact of voluntary codes of conduct, as well as previously cited anti-competitive concerns create the case for more active policy intervention. Policymakers in Brussels are planning a number of important interventions to bring further harmonisation and raise standards, but their precise level of ambition and areas of focus remains unspecified and fast-evolving. Targeted correctly, the Data Act and Digital Markets Act offer an opportunity to correct existing shortcomings, further harmonisation of the EU market and seize value from industrial data.

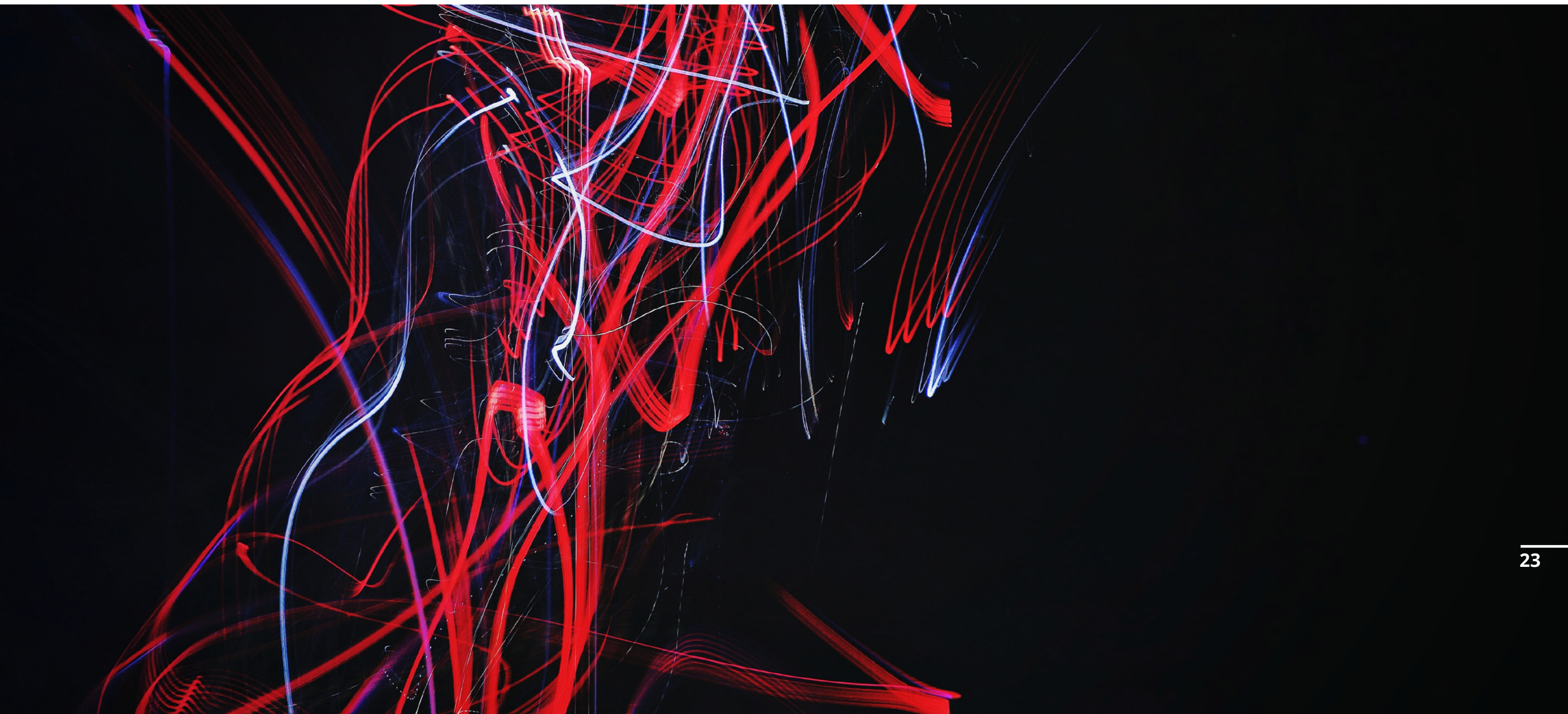
But EU institutions must move fast. Different sets of policy schemes and certifications are emerging across EU Member States. For example, certain Member States are choosing to emphasise the need for immunity from non-EU legislation, when the EC has itself decided to extend the free movement of data principles to jurisdictions that demonstrate adequacy in terms of data protection, like the UK or Switzerland. Such discrepancies generate legal uncertainty regarding what constitutes a 'sovereign' solution within the EU, and accentuates market fragmentation. This is likely to slow down adoption of cloud-edge solutions by European organisations, particularly in sectors with stricter requirements, and further hamper the ability of EU businesses – providers and users – to achieve the economies of scale required to succeed in the data economy. Such approaches also downplay the assurances brought by recent advances in encryption of data in the cloud, which can prevent access to customers' data both by cloud providers and unauthorised third parties in a cost-effective manner. Several large private EU organisations are already going in this direction, as illustrated by the example of Deutsche Bank's recent announcements in Chapter 3.

More widely, the current policy debate creates confusion and fuels calls for protectionism by seeking to address very different policy objectives – growth of the data economy, competition, data protection, use of cloud in public and critical infrastructure sectors – all under the banner of 'data sovereignty'.

Favouring exclusion over regulation of non-EU providers will significantly reduce market diversity, and shut out European users from access to global best-in-class technologies.

It would also reduce European cloud service providers' exposure to international competition, likely compromising their competitiveness on the global stage. Moreover, it would significantly hamper European industrial leaders' ambitions to scale outside of Europe if their applications, devices and data are not natively compatible with or portable to the de-facto standard cloud infrastructures abroad.

Conscious of this risk, the construct of national policy schemes like France's "cloud de confiance" doctrine implicitly incentivises the emergence of two types of roles in the market for public sector and critical infrastructure: that of 'trusted European operators', and that of global best-in-class technology provider. In recent months, a handful of partnerships between EU and non-EU players have emerged to attempt this new model. Such partnerships are another one of the new models explored in the following chapter.



CHAPTER 3
UNPACKING THE DYNAMICS IN EUROPEAN SUPPLY & DEMAND FOR "SOVEREIGN" CLOUD-EDGE SOLUTIONS

As laid out in previous chapters, cloud and edge computing offer significant growth and innovation opportunities for the European market, but the status quo raises several concerns. A raft of policies are emerging at EU and national level to seize these opportunities and address these concerns – conflated under the umbrella of achieving 'sovereignty' in the cloud-edge domain.

But to what extent do the policy debate and proposed measures to achieve data sovereignty match concerns of the end-users they seek to serve? What impacts are they having, or expected to have, on demand and supply for cloud services in Europe?

The present chapter unpacks the notion of sovereignty from end-users' perspective, thanks to exclusive data obtained from surveys conducted in May-June and November 2021 with over 600 senior executives of EU-based public and private organisations[39].

It also reviews the way providers are innovating to meet varied and at times uncertain customer and policy requirements associated with sovereignty, illustrating the trends with a selection of provider and end-user case studies

Insights drawn from this analysis are used later in the study to project the impacts of different policy scenarios (chapter 4) and inform the best course of action for EU and national regulators (chapter 5).

UNDERSTANDING SOVEREIGNTY FROM THE PERSPECTIVE OF EU ORGANISATIONS: WHAT DO END-USERS SEEK FROM THE MARKET?

With almost 90% of EU organisations surveyed being familiar with matters relating to data and technological sovereignty, there is no doubt that the debate around sovereignty has gained in prominence across European industry. The debate is fuelled, on one hand, by the growing use of cloud in recent years, and the critical role that digital technology has played in tackling the Covid crisis and seeking new sources of growth, and on the other hand, by the emerging EU and National level requirements as laid out in chapter 2. In this context, we asked end-users what benefits they most expect from sovereign solutions. The answers provided reflect a multi-faceted definition of sovereignty.

[39] *Public organisations represented 11% of respondents. Private organisations included SMES with >50 m€ turnover.*

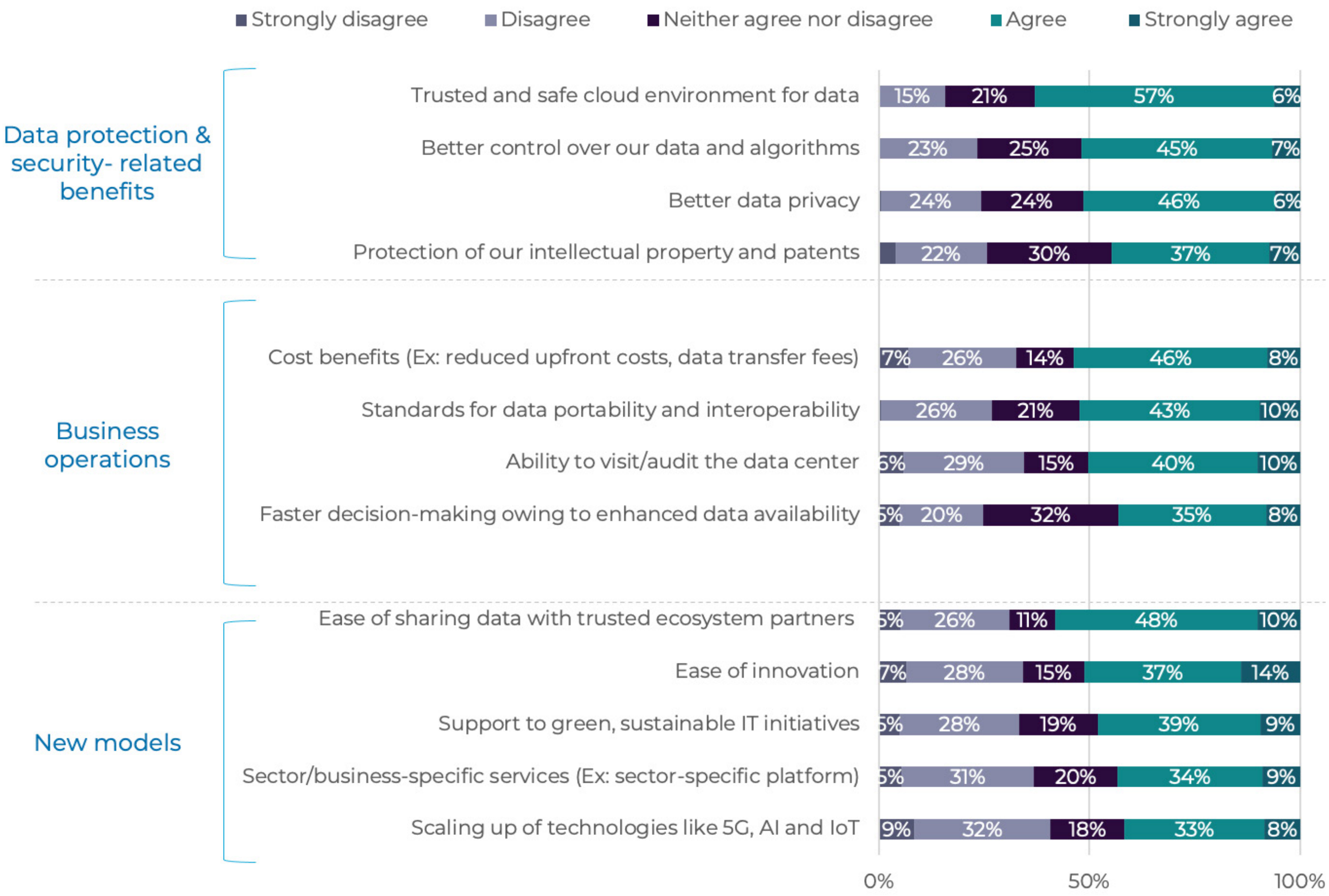


FIGURE 7: Key benefits expected from a "sovereign" cloud-edge solution amongst EU-based private & public organisations

When defining a "sovereign" cloud-edge solution, organizations primarily value trust, control but also greater ease of collaboration with their business ecosystem. Such organisations seek end-to-end services that combine best of breed solutions for

- **Data protection and security related benefits:** allowing organisations to keep control of their data and algorithms in a trusted and safe cloud, to guarantee better data privacy, and to protect their intellectual property.

- **Business Operations:** allowing organizations to have visibility of and control over their cloud service provider's operations while enabling better informed business decisions, increasing collaboration opportunities, and reducing costs.

- **New business models:** allowing opportunities to share data and services with a trusted ecosystem of partners and collaborate across sectors with greater ease , accelerating innovation, developing sector specific services, and scaling of new technologies and greener IT

This latter aspect is particularly interesting: it points to strong underlying expectations in terms of ability to develop business models that inherently require multi-cloud interoperability and suggests that private sector support for European sovereignty in the cloud-edge domain actually crystallizes a very diverse range of user demands, far beyond traditional concerns around data security or legal sovereignty.

THE DETERMINANTS OF TRUST IN CLOUD-EDGE SOLUTIONS

Still, trust in providers remains the key factor. In fact, more than 84% of EU organisations are very likely to favour a CSP that meets their requirements in terms of trust. So the question becomes: what do end-users mean by trust? What are the attributes that they most associate with a cloud solution that meets their requirements for trust?

First, it is important to underline that EU organisations consistently associate a wide set of technical, operational, and legal attributes in their definition of what constitutes a "trusted" cloud solution, as shown by the figure below.[40]

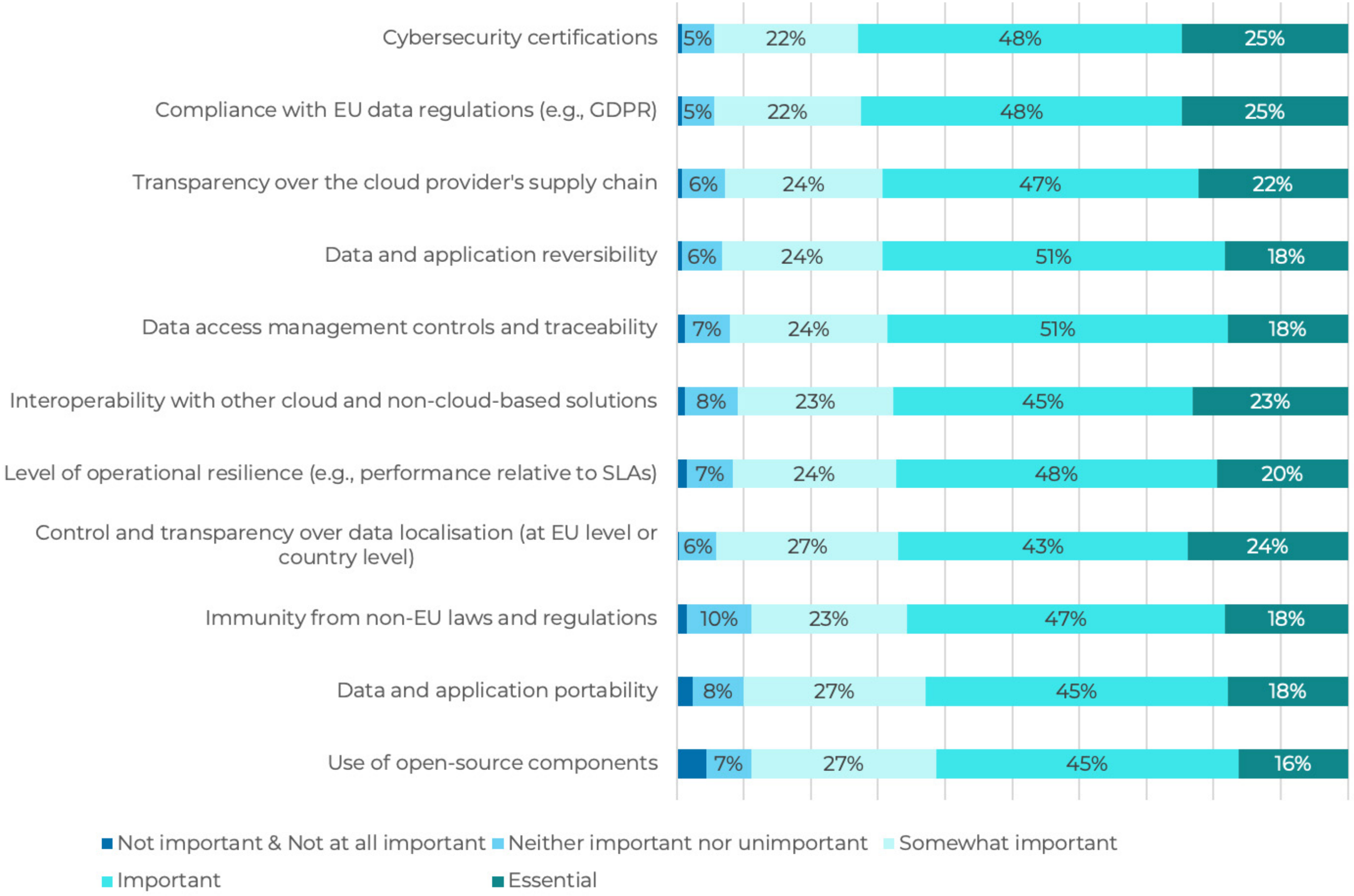


FIGURE 8: The determinants of trust in a cloud-edge provider amongst EU-based private & public organisations

[40] *Requirements shown in figure 8 were ranked as important or essential by more than 50% of respondents.*

Overall, end users are demanding more options for the way their data is handled, secured, and turned into value for their business. The market must move fast to address these needs or face disruption, penalties, or worse. Not all industries have adopted cloud-edge at the same rate and there are certain sectors that have become early adopters; the best examples of these lie within the software and technology industry. Being an early adopter has meant realising benefits early but has also come with its own challenges.

Among the many operational dimensions that were put to the organisations surveyed, cybersecurity certifications, compliance with EU regulations and transparency over the cloud providers supply chain top the list of essential or important requirements. These stress the focus that organisations put on guaranteeing compliance with regulatory requirements and minimising legal risks. Additional dimensions such as reversibility, interoperability and portability reflect the importance organisations put on their freedom to choose the most appropriate solution and migrate their data and operations to it seamlessly. Other aspects such as data access management controls, operational resilience and use of open-source components focus on their demand for control and autonomy.

Immunity from non-EU law also ranks among the parameters that certain EU organisations attribute with trusted cloud-edge solutions[41]. More in-depth discussions with senior executives of EU organisations indicate that, in practice, many of these organisations actually seek “immunity” to avoid the risk (perceived or otherwise) of legal uncertainty rather than to avoid non-EU technology providers. These senior executives share that they especially wish to minimize any operational risk of having to cease using certain providers overnight due to shifts in law or regulation, such as that which occurred with the ECJ’s Schrems II ruling.[42] This finding has important implications for future EU rule-making in this area, which are addressed further in chapter 5.

[41] To understand the potential reasons as to why this parameter resonates with certain survey respondents, it is important to recall the impact that US sanctions on banks like BNP Paribas – fined $8.9 billion in 2015 for transactions with countries under US sanctions, based on the fact parts of the transactions had taken place in US dollars – and Deutsche Bank – fined on similar grounds in 2015 and 2020 – have played in making European industry bosses fearsome of the extraterritoriality of US law. It is also the case that it is topic that has tended to capture headlines, therefore creating a certain level of exposure and awareness in the market.

[42] Certain organisations also seek immunity to protect the economic value of their data, but this appears to be based on unproven fears that extraterritorial US legislation could also be distorted to facilitate economic espionage.

The importance of legal certainty

After delaying their transition to cloud-based solutions, primarily due to the complexity of their data and perceived security risks of hosting data in a public cloud, many European telecommunication operators have initiated a phased move of their data assets to the cloud as a means of generating new value and remaining competitive.

A mid-sized EU based telecommunication player interviewed for this study engaged on this path in partnership with a leading global hyperscaler. Yet, in 2021 the firm chose to revisit its move to the cloud in the face of legal uncertainties resulting from the ECJ's Schrems II decision as well as the fast-changing nature of requirements emerging across Member States. While the telecommunication player considered it has gained sufficient assurances to prevent illicit access to its data, thanks to the latest types of encryption implemented by the cloud provider, it judged that the sum of reputational, operational and legal risks involved with adopting the public cloud solution that met its needs was too high.

Moving forwards, it has chosen to opt in the short term for a private cloud solution, considering that alternative public cloud solutions on the EU market did not offer sufficient value relative to its needs and identified risks. In the mid to long term, they could reconsider a more significant move to the cloud in the face of greater regulatory certainty, if the current architecture were to slow down their ability to develop and scale new data services.

However, when asked to rank all the elements above, organisations are most likely to prioritise cybersecurity certifications, compliance with EU law, control over data localisation and interoperability in their choice of provider.

In practice, trust needs to be put in the balance with other key factors of choice, like cost, to measure its relative importance to users. Measuring the trade-off EU organisations are willing to make between trust and price shows that EU organisations are willing to pay extra for trust. This is especially true if the price difference can be contained below a 10% surplus relative to global market average – at which price point the number of EU organisations willing to choose cloud-based solutions increases compared to today's situation. At this premium, the EU market's ability to meet users' diverse requirements in terms of trust is therefore likely to increase adoption of cloud-based solutions.

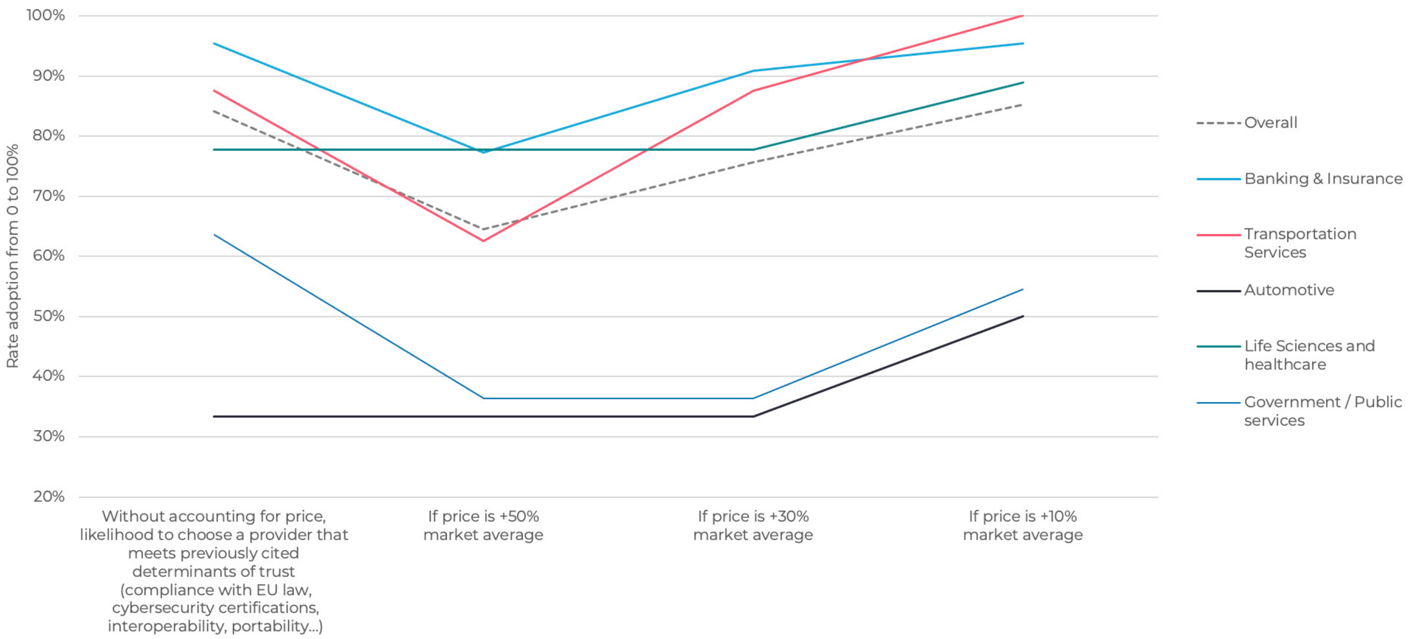


FIGURE 9: *Measuring the trade-off between trust and price for EU organisations through their likelihood to choose a cloud provider*

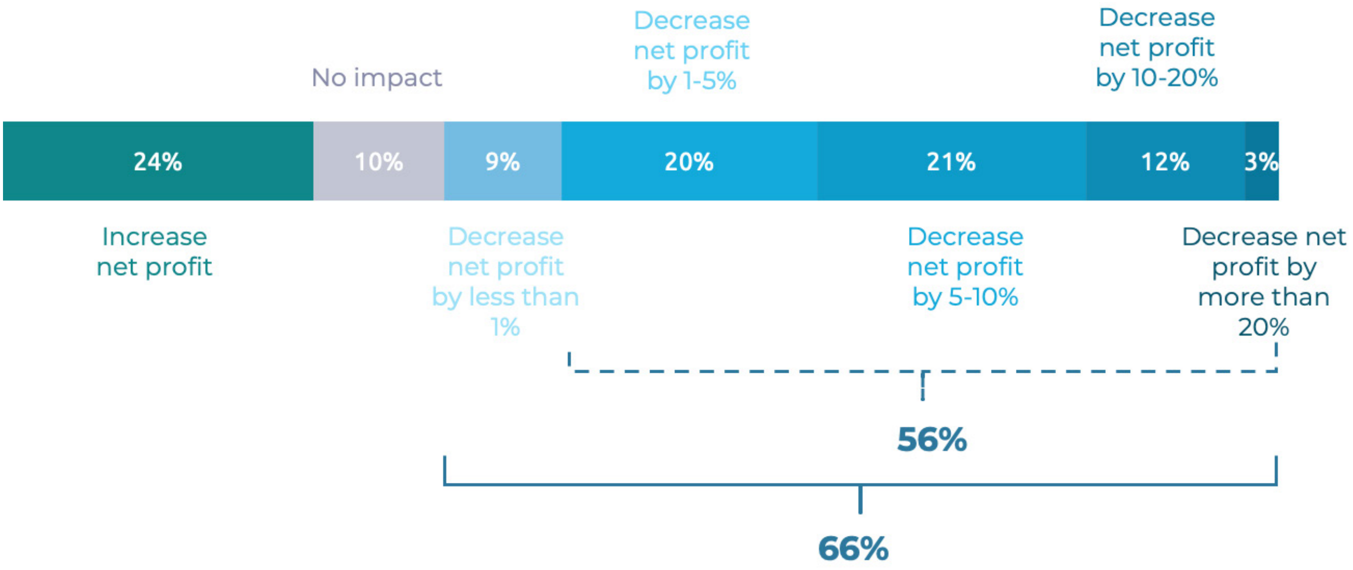


FIGURE 9: Expected financial impact of a ban on use of non-EU cloud providers measured as impact on net profit (or on budget targets if non-profit), if given 24 months' notice

Choice is however likely to remain key, and bans on non-EU based providers, as touted by certain European policymakers and certain industry players, are likely to have a significant negative impact on EU organisations. In fact, 66% of organisations surveyed as part of the present study consider that a ban on non-EU providers would impact their financial forecasts, even if given 24 months' notice before the ban comes into force. The survey respondents who indicated that such a ban would likely increase their net profits were primarily players in the technology industry, therefore prone to consider non-EU players as competitors.

Like other operational considerations within the field of trust (such as cybersecurity or network connectivity) organisations must achieve a balance for investment in servicing data with other strategic priorities. There is a cost associated with creating and maintaining trusted solutions, and whilst cloud edge players can absorb some of the impact through considered partnerships and flexible offerings, often the costs filter down to the user.

END-USERS' PERSPECTIVE: THE BOTTOM LINE

Data and cloud sovereignty is by now clearly on the agenda of many organisations. Trust in the ability of their CSPs to abide by the relevant cybersecurity certifications, to comply with EU law is their utmost concern. They also strongly value CSPs that guarantee control over the localisation of their data as well as choice and flexibility through enhanced reversibility, portability, and interoperability. They are in fact prepared to pay a premium of up to 10% for offers that meet their diverse requirements in terms of trust – within this cost boundary, "trusted" cloud-edge solutions will likely result in an increased adoption of cloud-based solutions. This reflects a broader demand for choice which also includes their ability to carry on benefiting from the offers of non-EU providers.

The debate on European data sovereignty has also blurred the distinction between, on one hand, concerns over conflicts of laws particularly between the United States, China and the EU, and, on the other hand, concerns over Europe's competitiveness in the digital sector: in other words, between legal and economic perspectives of sovereignty. In the former, what matters is that organisations (and their providers) not be exposed to laws that could breach EU data law: being based in a jurisdiction that is covered by GDPR or considered adequate by EU institutions is sufficient. In the latter, the key is to make sure value is being created in Europe and supporting competitiveness of European businesses at home and abroad. But by conflating the two types of concerns, certain EU firms are assuming that they must resort to exclusively EU-based cloud-edge providers and data localisation to achieve regulatory compliance and gain a competitive advantage.

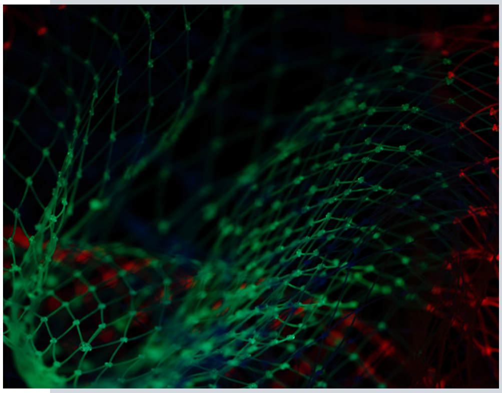
The end-users demand outlined in this chapter call for a regulatory framework yielding the desired supply of cloud-edge solutions. Three such policy scenarios are defined in the next chapter and compared in terms of the adoption of cloud-edge solutions and the resulting economic benefits for each of them.

HOW ARE PROVIDERS MEETING THESE NEEDS WITHIN EUROPE?
NEW MODELS

Novel approaches are emerging across Europe to address evolving user and national policy requirements in terms of data protection, interoperability as well as industry-specificity. The case studies below give a flavour of the types of solutions likely to become available in coming years.

Insufficient clarity, stringency, and harmonization of requirements across Member States could however limit providers' ability to distinguish their value proposition and/or benefit from economies of scale at EU level.

What is "industrial data"?



Several European banks have substantially restricted the scope of their move to cloud and have partnered with on premise data centre providers. This is increasing the time to market and the cost of the development of their data and AI services. To make up for this loss of competitiveness, some creative initiatives have recently brought together European banks and American hyperscalers. For example, Deutsche Bank has recently announced a partnership with GCP. This partnership aiming to "use data more intelligently and provide a flexible and safe environment [...] to quickly deliver new products and services" Bernd Leukert, Deutsche Bank's Chief Technology, Data and Innovation Officer and Member of the Management Board.

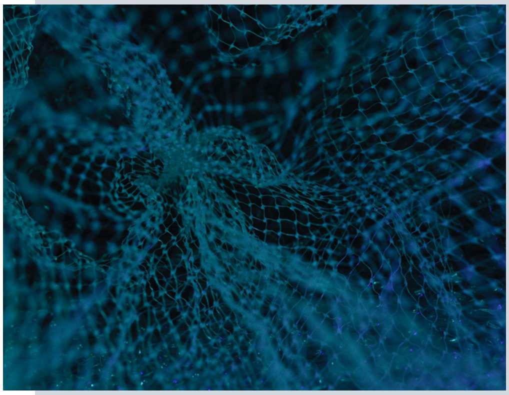
Benefits: *Data protection and security related benefits, Business operations*

New partnership models

National cloud doctrines, together with the ECJ's Schrems II decision, have spurred the emergence of new partnership models between EU-based players and global best-in-class technology providers. In France, Capgemini and Orange have announced plans to jointly create a new company called Bleu that will deliver Microsoft's Azure and Office 365 services in "Cloud de confiance" compliant environment. Similarly, OVHcloud, a French cloud provider has announced a partnership with Google to host its PaaS platform (called Anthos) on its EU-based private cloud infrastructure. Deutsche Telekom has announced a similar partnership with Google to serve the German market.

Benefits: *Data protection and security related benefits, Business operations*

Virtualisation and Containers

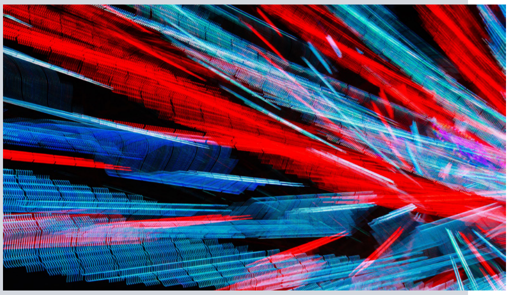


Following on from the virtualisation trend, containerisation has become an increasingly popular software development trend. The main implication of containerisation at a data sovereignty level, is that containers can be easily moved on and off the cloud, and moved between different clouds, allowing organisation to mitigate vendor lock in and to try different use cases with more ease by leveraging open source solutions through novel approaches such as accredited containers and Containers-as-a-Service (CaaS). These approaches promote and facilitate an increased collaboration in developing software solutions while guaranteeing a variety of properties of these solutions in terms of security, data localisation, interoperability and more. This opens up unique opportunities to collaborate and innovate in an open and trusted ecosystem. Here are some examples of CaaS uses:

- The Cloud Container Engine of the German Telekom's public cloud (the Open Telekom Cloud) is based on Docker and Kubernetes.
- CERN Manages over 300-thousand cores of OpenStack and more than 500 Kubernetes clusters using OpenStack Magnum.
- Ericsson uses cloud native and several open-source technologies including Kubernetes in their portfolio to address the needs of 5G networks.
- The U.S. Department of Defence (DoD) containerised their entire stack. To maintain global data interoperability, collaborating with their ecosystem through open-source development without being locked into a particular vendor. They coined the term of "accredited containers" to refer to such containers.

Benefits: *Data protection and security related benefits, Business operations, New business models*

Capturing the value of a multicloud strategy



In 2021, 92% of large organisations indicated they either had or were in the process of implementing a multicloud environment, and that they use, on average, 2.6 public and 2.7 private clouds. Part of this complexity is inherited through mergers and acquisitions, but in many cases organisations also actively choose to partner with multiple cloud service providers to benefit from a greater diversity of applications as well as reduced vendor lock-in. However, they then struggle to turn that diversity into tangible economic benefits.

In response to this growing trend, Kyndryl and Vodafone have partnered to provide customers with a one-stop-shop solution that simplifies the inherent complexity of multicloud. Vodafone's Business Multicloud Platform, based on Kyndryl's Multicloud Management Platform, allows organisations to directly manage their applications across multiple clouds through a single interface, while Kyndryl brings the skills and tools to design the most effective strategy and implement interoperability and portability in practice, i.e. by interconnecting the APIs of different providers. Thanks to this partnership, customers can come to Vodafone for end-to-end support, from implementation of tailored network, cloud and MEC solutions with different providers, to the ability to easily manage these services over time.

Kyndryl and Vodafone's experience shows that greater standardisation of services across providers, including APIs standards, would significantly reduce cost and increase ease of collaboration across platforms, unlocking more value for users.

Benefits: *Interoperability, Portability, Business operations*

GAIA-X: A MODEL FOR EUROPEAN DATA SOVEREIGNTY?

Formally launched in 2019, Gaia-X has quickly emerged as the most prominent industry initiative seeking to achieve European sovereignty in data infrastructure, cross-sector data exchange and data-service brokerage. As of early 2022, over 300 firms from all sectors have joined the organisation, which has also received strong political backing from German, French and Italian ministries of economy.

Gaia-X has three main areas of work. First, it seeks to develop a reference architecture and open-source technical standards for a “federated” approach to publishing, consuming, and verifying data and data-services among trusted participants. The view is that European data sovereignty is best achieved by facilitating interoperability between trusted cloud-edge infrastructure and data services, empowering data-owners with policies that govern the usage of their data, minimizing transfers of raw data, and only sharing data insights relevant to a given use case. Second, Gaia-X is developing a set of “policy rules” that seeks to fill the gap in EU-wide certification for trusted cloud services. In November 2021, it launched a consultation on its proposed Gaia-X Compliance & Labelling scheme, which distinguishes three levels of certification:

- ***Level 1*** *would be broadly equivalent to the cybersecurity standard being developed by ENISA*
- ***Level 2*** *extends level 1 with a mandatory option to be located in Europe*
- ***Level 3*** *adds “criteria that ensure immunity to non-European laws” yet allowing for a European location and operationalisation*

Thirdly, Gaia-X facilitates sector-specific working groups, tasked with aligning on use cases for data sharing and lead experimentations. The first proof-of-concepts are expected to see the light in 2022, but frustration has grown amongst members over the lack of practical advances to date. Whether they are active members of Gaia-X or interested bystanders, public and private decisionmakers interviewed for the purpose of this study all agree that Gaia-X’s top priority going forward should be to demonstrate the feasibility and value of interoperability standards and trusted data ecosystems, by moving away from policy rules and into practical experimentations. To this end, Gaia-X have run well-attended ‘Hackathons’ and developed a prototype data-brokerage portal[43]. Development work is open, transparent and undergoes formal public change control.

In recent months, Gaia-X has drawn criticism for admitting major US and Chinese technology providers within its members. Yet, the fact such major players are keen to join and abide by technical and policy standards driven by European industry[44] actually constitutes a significant achievement in interest of European sovereignty, and a testimony to the influence attained by Gaia-X over its short period of existence.

[43] *Results from these Hackathons are published here: https://hackathon.minimal-gaia-x.eu*
The prototype of Gaia-X data-brokerage portal is accessible here: https://portal.minimal-gaia-x.eu

[44] *Gaia-X’s governance rules do not allow non-EU organisations to sit on its Board of Directors.*

CHAPTER 4
MODELING THREE FUTURE POLICY SCENARIOS

Data and cloud sovereignty is often viewed as a topic focused on compliance and control. However, when unpacking the notion of sovereignty, there is much to be gained by regulating the market to foster offers that meet a wider and finer range of end-users requirements. To this end, the present study takes a demand-driven perspective incorporating what EU industry value most in a future cloud-edge market namely, a competitive ecosystem of "trusted" solutions offering an adequate protection of EU data, promoting the adoption of cloud-edge and interoperability through data ecosystems, and increasing EU organisations' competitiveness in the data economy.

The unfolding debate on cloud-edge sovereignty can lead to a wide range of supply-side interventions in the market as a consequence of the regulation that will be enacted over the next few years. To ground the debate and recommendations on achieving European cloud-edge sovereignty into an evidence-based analysis, the present chapter defines three policy scenarios and compares their outcomes in terms of the economic benefits they generate, exploring how different regulatory and industry initiatives could influence the trajectories that are emerging across Europe, as outlined in previous chapters. These stylised scenarios help to break down the actions that regulators and industry can take to influence the path forward and support the EU to reach the best outcome. The levers at our disposal to achieve the possible trajectories include trust, choice (market diversity), investment and, to an extent, adoption.

The future cloud-edge market will be shaped by the trade-offs between market forces, and a combination of national and EU regulations that could differ between the different sectors of the economy.

The three scenarios analysed are therefore not exclusive.

- **Scenario A**. A "globalised free market" scenario tantamount to the situation in 2021 favouring self-regulation and laissez-faire leading to an uneven adoption of cloud-edge between industries as a function of the importance they attach to trust.
- **Scenario B.** A "fortress Europe" scenario wherein member states and the EU drastically limit the presence of non-EU cloud-edge providers and invest public funds to promote local solutions leading to different layers of regulation, driven by European Commission and national capitals resulting in fragmentation.
- **Scenario C**. An "open strategic sovereignty" scenario where the emphasis is on regulating providers through ambitious and harmonized data regulations and EU-wide industry-driven standards that promote trusted and globally competitive solutions, rather than excluding cloud-edge providers based on criteria such as nationality or legal control.

The details of these three scenarios provided in the table below feature key factors such as the processing of personal data and high-value datasets; the type of mandates of interoperability, portability and reversibility; the nature of cybersecurity controls; and the levels of private and public investments. For a given scenario the net value it generates is calculated in terms of the extent to which it addresses the demands of EU organisations for each key factor derived from the survey.

Scenario		A “Globalised free market”	B “Fortress Europe”	C “Open Strategic Sovereignty”
Summary		Status quo from 2021 is continued, deepening the divide between industries based on the importance they attach to trust.	Bans on non-EU-based providers allow local firms to extend their market share but add significant constraints and uncertainty for users and global technology providers, resulting in lower adoption and a smaller overall market.	Ambitious and harmonized data regulations and industry-driven standards are adopted at EU-level, pushing the market to innovate and provide trusted, globally competitive solutions.
Approach		There is no coherent regulation addressing data sovereignty at the EU level. Within a scenario where this remains to be the case, the European market continues to operate as it sees fit. We will see some standardisation across some industries, and there will be localised ways of operating for each member state.	Policy makers implement strong mandates on transparency, control (e.g. in the name of immunity from non-EU law and regulation and interoperability). Within this scenario, Europe strengthens the local cloud edge market through investment in local players and regulation susbstantially limiting use of non-EU cloud providers.	Whilst there are other nuanced approaches, in the third scenario modelled here, the EU remains open to working with extra-territorial cloud providers and hyperscalers to realise the investment potential for European businesses but creates appropriate checks and balances. This approach requires an open attitude towards costs, requirements, and interoperability to create a market with diverse options and clear regulation.
Key features	Personal data and 'high value datasets'	Personal data and 'high value datasets' can be processed by all entities deemed compliant with existing regulation (e.g. GDPR), but these requirements remain open to interpretation and are inconsistently applied across industries and Member States.	Personal data and 'high value datasets' cannot be processed by non-EU based entities. Different layers of regulation are driven by European Commission and national capitals in regards to data sovereignty, resulting in fragmentation. Member States (MS) may enforce additional national requirements e.g., restrict cross-border data transfers between certain MS.	Personal data and 'high value datasets' can be processed by non-EU entities who have obtained a (newly created) EU-wide data protection and cybersecurity certification.
	Interoperability, portability and reversibility	There are no mandated requirements for interoperability, portability and reversibility. Ecosystems develop within some industries or markets that choose to adhere to specific guidelines (e.g. SWIPO[1]).	Portability and reversibility are required of all cloud-edge computing providers in EU. Interoperability is also mandated, but requirements are fragmented from country to country and top-down (i.e., not based on EU or global industry standards).	EU law introduces portability and interoperability requirements between cloud-edge services (at infrastructure, platform, and application level) based on standards set by industry. These are widely implemented by providers in EU, resulting in emergence of new players and increased diversity of supply.
	Cybersecurity controls	Cybersecurity controls are driven by private sector and international standards. Certain sectors or governments may choose to enforce specific standards, but these vary in scope and are not widely adopted.	Cybersecurity controls are driven by national governments. These vary in scope and drive offers to the strictest standards with a potential impact on the diversity of available offers and the cost of these.	Cybersecurity standards are driven by a harmonized certification scheme with common technical requirements across EU member states. Levels of assurance focus on the effective amount of legal, technical and operational control, security and resilience offered by providers relative to EU regulations.
	Private investment	Private investment is high but primarily driven by leading global cloud providers, resulting in increased market concentration.	By 2030, average cost of cloud-edge services increases by ~30% within the EU relative to global market.	By 2030, average cost of cloud services increases by less than 10% within EU relative to global market.
	Public investment	Public investment is comparatively low and focused on national initiatives.	Public investment in cloud-edge solutions is high (in excess of 20bn€) but exclusively directed at entities meeting strict ‘EU control’ requirements.	Public investment is high, supporting projects that meet EU standards and that are expected to be competitive on a global level.
Result		Users will continue to benefit from growth, but benefits and adoption will significantly diverge between industries and markets based on the strength of their requirements.	Fragmentation and level of constraints imposed on the market are likely to result in reduced innovation and high average cost due to lower economies of scale, despite stronger data sovereignty assurances.	Users will benefit from greater controls, cost efficiency and interoperability, portability, with the ability to combine technologies to match their specific needs.

FIGURE 11: *The approach, key features and results of three future policy scenarios*

Leveraging existing studies together with the results of the surveys conducted for the purpose of this report[45], the impact of each scenario is measured in terms of their impact on two key metrics:

- **(1)** cloud adoption – measured in extra percentage points relative to a baseline forecast of 68% of adoption by 2030, as a factor of trust in cloud-edge services, average cost of services and diversity of cloud-edge supply accessible to EU-based organisations.

- **(2)** value generated from collaboration within and across sectors and organisations, especially through data exchange within industrial data ecosystems. This is measured as a factor of interoperability and portability effectively observed by users between cloud-edge services commercialized within the EU, but also between such services and those commercialized outside of the EU market.

The level of adoption of cloud and edge computing services is influenced by the following factors

- Impact of trust on adoption relative to current projections. Returning to the determinants of trust amongst EU-based organisations laid out in figure 11 chapter 3, scenario A fails to meet users' expectations in all dimensions except for the level operational resilience. Scenarios B and C provide guarantees in terms of transparency, traceability, portability, reversibility, immunity from non-EU laws and regulations cybersecurity certifications. Although for the latter, scenario C will yield a harmonised EU-wide approach to cybersecurity while scenario A is more likely to result in a fragmented individual member-state led approach.

- Cost of the services: Scenario B will result in a higher cost of offering compared to Scenarios A and C where costs will deviate only marginally from today's costs. These additional costs reflect reduced economies of scale and competition as a consequence of reduced number of cloud-edge providers as well as the higher cost of stricter and fragmented security standards.

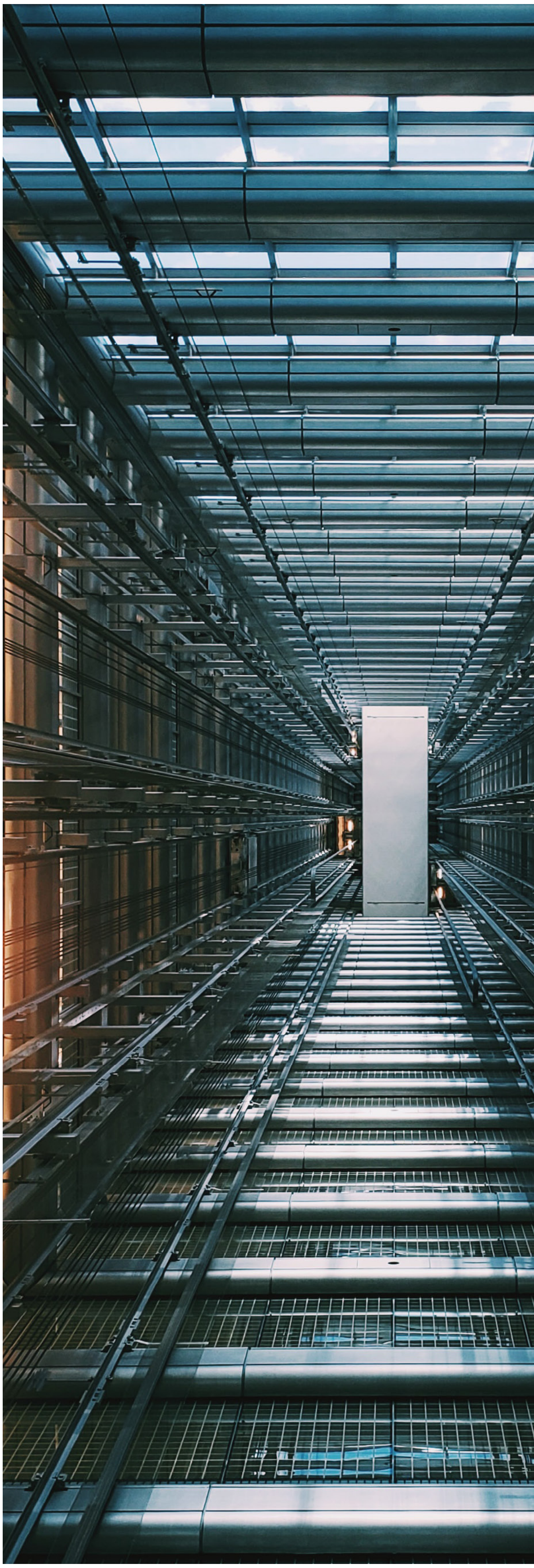
- Diversity of offerings: staring from today's 71% market share held by the three leading US hyperscalers, their future market share is determined by the characteristics of each the three scenarios in terms of the

- impact of regulation on diversity of offerings (specifically, regulation that forces infrastructure providers to open access to their data centres to turn infrastructure into utility), which will be high in Scenario B, moderate in Scenario C and low in Scenario A.

  » Public Investment in cloud supply-side, which will be high in Scenario B, moderate in Scenario C and low in Scenario A.

  » Private investment in cloud, which will be high in Scenario A, moderate in Scenario B and low in Scenario C.

Put simply, these three underlying metrics were chosen to measure users' willingness to adopt cloud-edge services based on the trust that users place in the cloud-edge services commercialized within the EU, the cost-effectiveness of these services, and users' ability to find an offer that meets their specific needs.



[45] *Data is derived from two surveys conducted by Capgemini with senior executives from EU as well as non-EU private and public organisations, conducted in May-June 2021 and in November 2021. The first survey encompassed 610 respondents from EU countries as well as 390 respondents from Australia, India, UK, US for comparison on specific questions. The second survey focused on a subset of 251 respondents from 13 EU countries. Respondents stemmed from public and private organisations across all sectors, including SMEs with >50 m€ turnover. Public organisations represent 11% of respondents. A small number of survey responses led to follow-up interviews with respondents. Additional data and reference points are drawn from publicly available studies and resources referenced in the Appendix.*

	By 2030...			
	Baseline adoption forecast (%)	68.0		
Weighted* impact on adoption of...	Users' trust in cloud-edge supply (range, % points)	-2.0 ●–● -3.0	7.6 ●–● 11.3	8.0 ●–● 12.1
	Average cost of solutions (range, % points)	0.8 ●–● 1.2	-2.6 ●–● -3.8	0.3 ●–● 0.4
	Diversity of cloud-edge supply (range, % points)	-0.5 ●–● -0.8	-3.6 ●–● -5.4	1.3 ●–● 1.9
	Projected impact on cloud-edge adoption by 2030 (range, % points)	**-1.7 ●–● -2.5**	**1.4 ●–● 2.1**	**9.6 ●–● 14.5**
	Projected cloud-edge adoption by 2030 (range, %)	**65.5 ●–● 66.3**	**69.4 ●–● 70.1**	**77.6 ●–● 82.5**
	Potential extra value generated thanks to increased data exchange and collaboration across sectors and organisations (range, Bn €)	**97 ●–● 117**	**198 ●–● 244**	**443 ●–● 576**

FIGURE 12: *Net value generated from each scenario by 2030. Due to impacts on trust, cost, diversity of supply and interoperability*

The outcome of the analysis for the 3 scenarios is that

- Trust is vital in driving cloud adoption with scenarios B ("Fortress Europe") and C ("Open Strategic Sovereignty") providing the regulatory certainty and the transparency levels sought after by users, particularly in market segments like the public sector, critical infrastructure or aerospace-defense that have lagged behind in cloud adoption.

- The increased average cost and the net reduction in diversity of the available solutions, due to the blanket exclusion from the EU market of providers on the basis of location of headquarters and legal owners and control, outweighs the trust benefits in scenario B.

- Scenario C ("Open strategic sovereignty") provides the highest adoption rates as a function of trust and diversity of offering as well as further benefits to the data ecosystem through great portability and interoperability.

These factors combine into a net benefit of open strategic sovereignty that ranges between 9.6 – 14.5 additional percentage points of cloud adoption across the continent by 2030 relative to the baseline forecast – 12 more points than the next best scenario. The added benefits of this scenario in terms of interoperability and portability could generate up to 576 billion euros in extra value for EU organisations from industrial data exchange and collaboration within and across sectors – or up to 2.4 times more value than the next best scenario.

CHAPTER 5
RECOMMENDATIONS FOR POLICY AND INDUSTRY

Building on insights drawn from all previous chapters, this last chapter presents a consolidated view of the policy objectives that European leaders should prioritise to maximise overall value generated from cloud-edge services within the EU and enable competitiveness of European industry in the global data economy, while ensuring adequate protection of their data. It then lays out paths towards those outcomes, in the form of recommendations for upcoming EU regulatory interventions as well as best practices for industry.

CHARACTERISTICS OF AN IDEAL EUROPEAN SOVEREIGN CLOUD-EDGE POLICY TEMPLATE

As laid out in previous chapters, sovereignty is a multi-faceted concept. Achieving Open Strategic Sovereignty in the cloud-edge domain means achieving:

- economic sovereignty – by safeguarding rights but also practical ability of EU organisations to capitalise on the economic value of their data but also by ensuring competitiveness of European industry in the global data economy
- operational sovereignty – by ensuring that EU organisations retain operational control over their data and applications in the cloud-edge domain through adequate cybersecurity and traceability, as well as interoperability and portability
- legal sovereignty – by ensuring that cloud-edge solutions used by EU data organisations fully comply with EU law, like GPDR (and are not superseded by laws of third countries)

Moreover, sovereignty is an empty concept if it does not deliver value, which is why industrial policy should also seek to maximize the value generated from cloud-edge solutions.
To this end, policymakers must seek to achieve a balance between the following underlying parameters:

- Broad adoption of cloud-edge solutions across all types of sectors (from consumer goods to organisations critical to national security) by ensuring that the market serves the market's diverse set of expectations in terms of trust, depth of services as well as total cost incurred by end users
- A diverse supply of solutions consistent with Open Strategic Sovereignty promoted through fair competition amongst cloud-edge providers, as well as by regulating rather than excluding cloud-edge service providers from the EU market.
- An environment that favours investment and innovation by technology providers, enabled through economies of scale for players that make the effort to meet EU requirements thanks to harmonised regulatory requirements within the EU, as well as through support to private investments in innovative solutions made within the EU, particularly in relation to multi-cloud and multi-edge interoperability.

RECOMMENDATIONS FOR POLICY MAKERS ON THE BEST PATHWAY TOWARDS A TRUSTED EDGE-CLOUD ECOSYSTEM IN EUROPE

To deliver on this ambition, European policymakers should look to the following recommendations. The policy proposals being developed by the European Commission (EU Data Act, EU Cloud Marketplace) and European Cybersecurity Agency (ENISA European Cybersecurity Certification Scheme for Cloud Services, or EUCS)) are expected to make several steps in this direction and as such are best fit to fully implement these recommendations.

Recommendation #1: Align on a harmonised definition of trusted cloud-edge services at EU-level that provides clarity to users and providers regarding the technical and operational requirements that must be met by cloud providers to be fully compliant with EU law.

Based on current law and previously outlined key outcomes prioritised for EU cloud policy, European policymakers should endorse a definition of trusted cloud-edge services that secures cross-border data flows within the single market, as well as with jurisdictions whose data protection frameworks have been granted adequacy status by the European Commission under GDPR. Access to national markets and public procurement for cloud services should remain non-discriminatory, and compliant with EU and WTO law.

This would enable economies of scale and competition across a wide number of providers and geographies, while achieving the legal certainty required by users to adopt cloud. Demonstration of material economic activities in the EU by providers could also be required, in order to further boost the EU's weight in the global data economy.

Recommendation #2: Expedite the implementation of a pan-EU framework for cloud certification and a publicly accessible EU-wide 'registry' of EU-certified cloud-edge solutions.

To promote trust, clarity and guard against market fragmentation, the definition in recommendation #1 should be at the heart of an EU-wide certification mechanism for cloud and edge services. Certifications would be granted for a given service, based on the effective amount of legal, technical, and operational control, security and resilience offered to users relative to EU law, and in line with the requirements compiled in the EU Cloud Rulebook. The purpose of this certification scheme is to meet specific 'sovereignty' assurances required by organisations in the public and critical infrastructure sector – its use by organisations in other sectors would remain voluntary to avoid creating any unnecessary burden, as per current policy in Member States with existing cybersecurity certifications, and proposals being developed by ENISA.

Any provider that meets the requirements of the pan-EU certification should be free to offer cloud-edge services in any European Member State once they have been certified rather than having to certify their services in each Member State.

Such a scheme would also improve access to trusted cloud-edge solutions for EU-based organizations across all sectors, thereby unlocking further adoption.

The registry of EU-compliant cloud-edge services could be a key component and strong source of value of the EC's planned 'European cloud marketplace'[46].

[46] *For a more detailed scoping analysis and set of recommendations for the EC's planned European cloud marketplace, see: https://digital-strategy.ec.europa.eu/en/library/building-european-cloud-marketplace-conceptualisation-study*

Recommendation #3: Introduce fit-for-purpose regulatory oversight in the market for cloud-edge services to promote fair competition and fair distribution of value towards end-users across EU industries.

National regulators for electronic communications appear best fit to fill the existing regulatory vacuum across the EU. They should be granted clear jurisdiction and responsibilities to promote competition in cloud-edge markets in the interests of end-users.

These authorities should leverage the experience they have in promoting competition and protecting end-users in electronic communications markets to address the current competition issues evident in the European cloud market (see chapter 2), and take a leading role in implementing recommendations #4.

This work should be complemented by the forthcoming Digital Markets Act, which will promote fairness and contestability in digital markets (with the Commission taking a central role in enforcement, with support from national regulatory authorities). It is vital that cloud services are within scope of the DMA, and that business users are able to take full advantage of new obligations upon digital gatekeepers to grant data access and portability and support interoperability with rival services.

Recommendation #4: Strengthen existing EU regulation by adding obligations that favour a more competitive, transparent and innovative market, harmonised at EU level.

European policymakers should seize the opportunity of the EU Data Act to introduce new, harmonised requirements to promote data and application portability across cloud-edge providers. Such requirements would move beyond the voluntary nature of existing codes of conduct (e.g. SWIPO), akin to the way that telecommunications operators are obliged to enable users to switch providers and that the European Electronic Communications Code already promotes the use of eSIM and 'over the air' switching solutions.

Working with industry, policymakers should also promote adoption of innovative new models to enable interoperability. This especially includes development of industry-driven standards that facilitate a federated approach to multi-cloud and multi-edge interoperability, as currently in development by Gaia-X. It can also materialize via the common use accredited containers, as discussed in the case study "virtualisation and containers").

Furthermore, appropriate regulatory measures should be introduced to increase the transparency of pricing by the existing cloud providers who have very strong market positions.

To ensure proportionality of requirements relative to wider policy goals of adoption and competitiveness of European solutions on the global stage, policymakers should seek to limit the "extra cost of an EU trusted service" to up to 10% relative to solutions on the global market when designing the above regulatory requirements and guidelines[47].

Recommendation #5: Promote investment in sovereign cloud-edge solutions in a manner consistent with abovementioned recommendations and that leverage "federated architecture" principles as promoted by Gaia-X to meet users' data localisation requirements while maintaining free flow of data across approved jurisdictions.

Investments should particularly be targeted at solutions in areas that present a distinctive opportunity for European competitiveness in the data economy, such as edge computing and higher return "up the stack" services such as AI, PaaS and cross-provider interoperability solutions rather than physical data centres.

This can be achieved by:

- making use of available funding such as the Digital Europe Program (DEP), Horizon Europe (HE), Connecting Europe Facility (CEF2), and Important Projects of Common European Interest (IPCEI) for developing and deploying sovereign cloud-edge solutions that meet different levels of expectations in terms of "trust" and compliance at a tolerable cost.
- allowing providers to participate in EU funded projects as long as activities take place in the EU, are compliant with EU law and that organisations provide the necessary guarantees and, i.e. are based in EEA or in jurisdictions whose regulations provide equivalent protections for handling of personal data, as affirmed by adequacy decisions of the European Commission.

[47] This metric is drawn from price sensitivity analysis conducted in this study (see Chapter 3). In practice, this could be assessed via a regulatory impact assessment carried out in conjunction with new rule-making.

APPENDIX

QUANTITATIVE ANALYSIS METHODOLOGY & SUPPORTING EVIDENCE

Methodology

The quantitative analysis model was built to estimate the impacts of three policy scenarios on two key metrics by 2030: projected levels of adoption of cloud solutions, and value generated from data exchange and collaboration within and across organisations thanks to increased interoperability of cloud-based solutions and data.

The three reference scenarios are outlined in figure 11 of the report (see Chapter 4).

In this model, based on the research and surveys compiled for the purpose of this study, adoption of cloud-based solutions within the EU market is assumed to be driven by three core variables:

- ***Level of trust in available service offerings*** (weight: 40%)
  As demonstrated in the report, trust is a multi-faceted factor, and encompasses users' considerations in regards to the below determinants in each policy scenario:
  - Interoperability with other cloud and non-cloud-based solutions
  - Data and application portability
  - Data and application reversibility
  - Choice and transparency over data localization (at EU level or country level)
  - Data access management controls and traceability
  - Compliance with EU data regulations (e.g., GDPR)
  - Immunity from non-EU laws and regulations
  - Level of operational resilience (e.g., performance relative to SLAs)
  - Use of open-source components
  - Cybersecurity certifications
  - Transparency over the cloud provider's supply chain

Based on survey results, each of these determinants is weighted according to the importance afforded by EU organisations ("average sentiment" in table 1.4 below).

- ***Average cost of cloud-edge services commercialized within the EU market*** (weight: 40%)
  For the sake of simplicity, the model looks at the impacts of the different scenarios on this average cost relative to global averages by 2030.

- ***Ability for users to find service offerings that match their needs, computed based on the forecasted effect of policy scenarios on the diversity, variability of offers, as well as ease of comparison by users'*** (weight: 20%)
  This last factor is driven by the following parameters:
  - Regulation, including the scope of providers allowed to compete in the EU market
  - Public investment
  - Private investment

These factors are combined in the economic model to estimate the projected cloud edge adoption percentage in 2030, given that the projected baseline is 68%.

Separately, the extra value generated from interoperability through industrial data sharing ecosystems is derived as the product of three related parameters: (1) projected total EBITDA in EU27 by 2030, (2) projected EBITDA impact of cloud adoption, (3) projected percentage of total adoption (baseline adoption plus the scenario specific extra adoption) of cloud and edge computing services for each of the three scenarios, (4) potential extra value from data interoperability.

Estimating the net value

The economic model translates the characteristics of the three scenarios (table 1.1) into a set of quantitative variables that estimate the cost of cloud edge services, the diversity of service offerings and the adoption due the confidence of end users in the ability of the scenarios to meet the expectations laid out above. These are in turn combined to estimate the net value for each scenario.

Scenario	Description *Table 1.1*
Scenario A.	A ***"globalised free market"*** tantamount to the situation in 2021 favouring self-regulation and laissez-faire leading to an uneven adoption of cloud-edge between industries as a function of the importance they attach to trust
Scenario A.	A ***"fortress Europe"*** scenario wherein member states and the EU drastically limit the presence of non-EU cloud-edge providers and invest public funds to promote local solutions leading to different layers of regulation, driven by European Commission and national capitals resulting in fragmentation.
Scenario A.	An ***"open strategic sovereignty"*** scenario where the emphasis is on regulating to promote trusted and globally competitive solutions through ambitious and harmonized data regulations and EU-wide industry-driven standards rather than excluding cloud-edge providers based on criteria such as nationality or legal control.

The three value drivers listed and described below (table 1.2) have been identified as most relevant to data sovereignty and ultimately the net value for end users in each scenario.

Value driver	Description *Table 1.2*
Projected adoption	An input variable to net value, this calculates a percentage value for projected adoption in each scenario based on 4 factors as described above.
Diversity of offerings	An input variable to calculating projected adoption. This percentage represents the impact that the diversity of offerings within each scenario is expected to have on adoption.
Level of trust	An input variable to calculating projected adoption, this section looks at each scenario and produces a trust scoring across 11 factors described above.

The net value was calculated for each scenario using the same baseline of cloud adoption across scenarios. The figure (table 1.3) below, provides an overview of the contributing factors and data sources used for the cross-industry calculation.

Contributing factor	Scenario A	Scenario B	Scenario C	Source *Table 1.3*
Baseline *(equal across scenarios)*	68%	68%	68%	Forecasted based on Eurostat statistics: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Cloud_computing_-_statistics_on_the_use_by_enterprises
Projected extra adoption by 2030 *(%)*	1,8%	-2,4%	12,1%	Calculated based on survey sentiments on cost on adoption, impact of diversity of offerings on adoption, impact of trust on adoption and the impact of reduced opportunity due to the absence of non-EU players
Potential extra value from data sharing and interoperability *(% of revenue)*	4,7%	2,4%	9,4%	https://www.capgemini.com/wp-content/uploads/2021/07/Final-Web-Version-of-Report-Data-Ecosystems.pdf

In particular the estimate of the level of adoption and the extra value generated through data sharing are based on the extent to which each policy scenario meets end users' expectations as per survey results.

Survey data

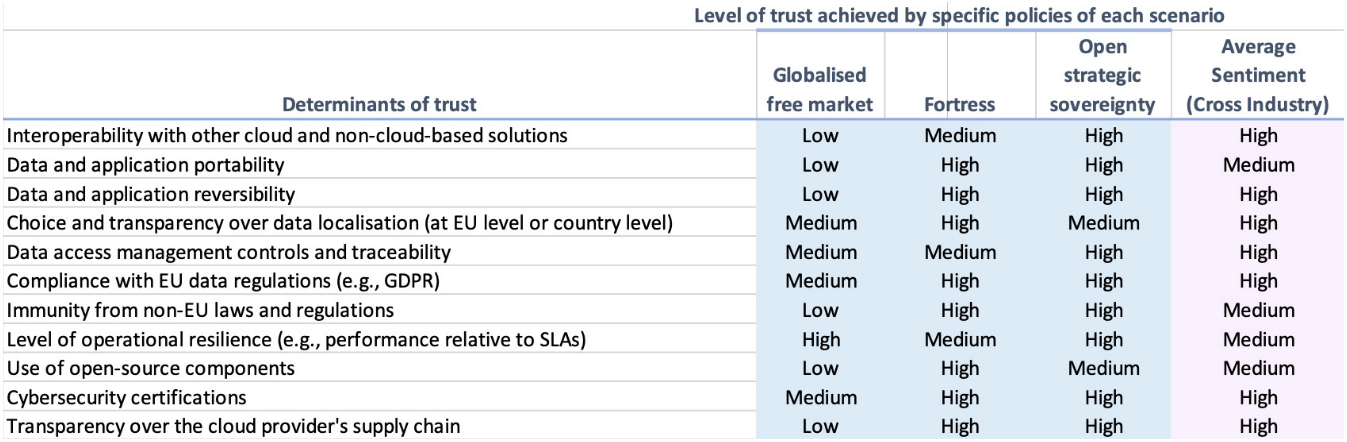
Two surveys were conducted among industrial leaders and subject matter experts on cloud edge across EU27 in automotive, government/public services, life science/healthcare and transportation services. The survey questions measure how public and private organizations in Europe define and prioritize data and cloud sovereignty. Participants were asked to rank the importance of the concepts for the level of trust they place in CSPs to gain an understanding of the trust sentiment users have for key concepts of sovereignty. The responses were used as input to our calculations to of the net value for end users.

In order to use the same survey data across the three scenarios in table 1.1, assumptions detailed below has been made:

- Each scenario is allocated a level (high, medium, low) against the area of trust
  - » For example, in the area interoperability with other cloud and non-cloud-based solutions scenario A is expected to have a medium amount of trust, scenario B a low level of trust and scenario C a high level of trust

- Participants were asked to give their sentiment of the importance of each area of trust to adoption

- A weighted sentiment score was used to calculate a quantitative variable that demonstrates an expected percentage increase / decrease per area and per scenario



	Level of trust achieved by specific policies of each scenario			
Determinants of trust	Globalised free market	Fortress	Open strategic sovereignty	Average Sentiment (Cross Industry)
Interoperability with other cloud and non-cloud-based solutions	Low	Medium	High	High
Data and application portability	Low	High	High	Medium
Data and application reversibility	Low	High	High	High
Choice and transparency over data localisation (at EU level or country level)	Medium	High	Medium	High
Data access management controls and traceability	Medium	Medium	High	High
Compliance with EU data regulations (e.g., GDPR)	Medium	High	High	High
Immunity from non-EU laws and regulations	Low	High	High	Medium
Level of operational resilience (e.g., performance relative to SLAs)	High	Medium	High	Medium
Use of open-source components	Low	High	Medium	Medium
Cybersecurity certifications	Medium	High	High	High
Transparency over the cloud provider's supply chain	Low	High	High	High

TABLE 1.4

The impact of diversity of offerings on adoption 2030 was calculated by:

- Measuring change relative to the current market concentration level, represented by the 71% market share currently held by the top 3 players (See Synergy Research, "European Cloud Providers Double in Size but Lose Market Share", September 2021).

- Adjusting the adoption level in each scenario to account for the impact on adoption of
  - » market concentration
  - » public Investment in cloud supply-side
  - » private Investment in cloud supply-side

These adjustments leveraged the sentiment in the survey in terms of the expectations of end users in terms of the factors determining trust, willingness to pay for a sovereign cloud solutions, and how each scenario meets these expectations.

ABOUT VODAFONE

Unique in its scale as the largest pan-European and African technology communications company, Vodafone transforms the way we live and work through its innovation, technology, connectivity, platforms, products and services. Vodafone operates mobile and fixed networks in 21 countries, and partners with mobile networks in 52 more. Our purpose is to connect for a better future, enabling an inclusive and sustainable digital society. Vodafone proactively works to expand access to connectivity for rural communities, students and jobseekers. For more than 30 years, Vodafone's Foundation has supported communities in Europe and Africa in the areas of health, education, and equality.

We support diversity and inclusion through our maternity and parental leave policies, empowering women through connectivity and improving access to education and digital skills for women, girls, and society at large. We are respectful of all individuals, irrespective of race, ethnicity, disability, age, sexual orientation, gender identity, belief, culture or religion.

For more information, please visit **www.vodafone.com**, follow us on Twitter at **@VodafoneGroup** or connect with us on **LinkedIn**.

ABOUT CAPGEMINI INVENT

As the digital innovation, design and transformation brand of the Capgemini Group, Capgemini Invent enables CxOs to envision and shape the future of their businesses. Located in more than 36 offices and 37 creative studios around the world, it comprises a 10,000+ strong team of strategists, data scientists, product and experience designers, brand experts and technologists who develop new digital services, products, experiences and business models for sustainable growth.

Capgemini Invent is an integral part of Capgemini, a global leader in partnering with companies to transform and manage their business by harnessing the power of technology. The Group is guided everyday by its purpose of unleashing human energy through technology for an inclusive and sustainable future. It is a responsible and diverse organization of 270,000 team members in nearly 50 countries. With its strong 50-year heritage and deep industry expertise, Capgemini is trusted by its clients to address the entire breadth of their business needs, from strategy and design to operations, fueled by the fast evolving and innovative world of cloud, data, AI, connectivity, software, digital engineering, and platforms. The Group reported in 2020 global revenues of €16 billion.

Get the Future You Want | **www.capgemini.com/invent**