analysys mason

Final report for Amazon Web Services – Executive Summary

The European telecoms regulatory framework: not a good fit for the public cloud

David Abecassis, Christopher Ryder, Nathan Williams, Laura Lechner, Rob Bratby

25 September 2024

Ref: 658783197-372

Contents of the full report

Analysys Mason Limited
North West Wing, Bush House
Aldwych
London WC2B 4PJ
UK
Tel: +44 (0)20 7395 9000
london@analysysmason.com
www.analysysmason.com
Registered in England and Wales No. 5177472

The full report is available at:
https://www.analysysmason.com/consulting/reports/eu-cloud-telecoms-regulation

Abstract

This paper contributes to the question, raised by the European Commission (EC) in its recent white paper on the future of digital infrastructure in Europe, of whether the cloud and telecoms sectors may be converging, to the extent that common regulation would be justified. Specifically, the EC outlines the option to expand the European Union (EU)'s telecoms regulatory framework to include cloud services. In this paper, we examine this question from a technical, legal and economic perspective, considering the history of the telecoms sector and the purpose for which the telecoms regulatory framework was constructed and implemented.

Cloud services allow European businesses to access IT building blocks running over distributed infrastructure. Public-cloud services are designed to be useable across industries, through common application programming interfaces (APIs). These services are underpinned by infrastructure that is distributed globally and connected via extensive private network links. European businesses benefit from cloud services financially, because they can access extensive IT resources with limited up-front investment and risk. They benefit operationally because they can access state-of-the-art IT building blocks, which very few businesses may have been able to source and access in a dedicated manner.

Businesses use cloud services through many independent software vendors (ISVs) which offer software on cloud platforms. This includes telecoms operators, which use cloud-based services offered by a range of vendors, most of which had been offering on-premises software for decades. Telecoms operators have begun migrating some of their non-network IT to public-cloud platforms, but migration of network IT remains very limited (less than 1% of workloads by some estimates), with no clear momentum towards greater use of the public cloud for network functions. The claims of 'convergence' are therefore at best premature, and at present largely inaccurate. Cloud providers and customers are indeed dependent on connectivity to be able to work together, but telecoms operators are likely to remain largely independent from cloud providers in the context of running their network. As they migrate network functions to the public cloud, they will do so using software-defined networking solutions provided by vendors such as Nokia and Ericsson, building on the same cloud services as are available to all other businesses.

Telecoms regulation (now under the European Electronic Communications Code, EECC) reflects a history of state-controlled monopolies, and the policy decision that regulation should support market liberalisation and competition. This translated into a strongly pro-competition ex-ante regulatory regime that required national regulatory authorities (NRAs) to review specific relevant markets and impose remedies on operators with significant market power, in addition to general conditions of authorisation. Interconnection between telecoms operators was and remains subject to regulation, reflecting the importance of direct network effects in traditional telecoms markets, in particular telephony.

By contrast, the cloud sector is relatively new, highly innovative and dynamic, with many providers competing for customers in different ways. Direct network effects are largely absent, but economies of scale are strong and not bound by national borders. The sector is already overseen through European competition law, and has recently been brought under the scope of new regulations including the Data Act, the Digital Market Act (for the largest providers), the Digital Services Act, and the revised Network and Information Security Directive (NIS2). Indeed, competition authorities have taken an interest in the competitive dynamics related to cloud services, and highlighted some concerns related to egress fees, barriers to switching and software licensing practices. If any regulatory concern is identified after testing these new instruments, regulators should seek to remedy them through proportionate and justified remedies, subject to a detailed impact assessment: the EECC was not constructed for this purpose and appears highly unlikely to be effective, justified and proportionate in addressing these potential remaining issues.

If the EC chooses to expand regulation to cloud services, it should conduct a detailed impact assessment. In the last section of the paper, we outline potential impacts for European cloud and telecoms providers, and end users in both sectors. We find that European cloud providers may face higher costs and reduced incentives for investments in Europe. Competition in the telecoms sector may be distorted in favour of larger operators, which have championed the regulation of IP interconnection as a way to extract payments to terminate internet traffic to their subscribers. Eventually, these effects would harm European businesses, affecting their ability to adopt, and benefit from, cloud and artificial intelligence (AI) services, which would be counterproductive to Europe's digital agenda and its ability to innovate through technology.

In conclusion, we reiterate the importance of well-functioning cloud and telecoms sectors to the digital agenda for Europe, and to the European businesses and public-sector organisations that use cloud services and stand to benefit from them, including in the context of AI and other highly innovative aspects of IT and digital technology. This is essential to Europe's competitiveness. Regulators should acknowledge the potential adverse impacts of extending the telecoms regulatory framework to encompass cloud services, without clear justification or assessment of its impacts. A nuanced approach, recognising the unique characteristics and dynamics of both sectors, is essential to avoid these risks and support continued growth and innovation for European businesses.

Executive summary

1 Introduction

Cloud services are central to Europe's digital transformation. Businesses are increasingly migrating some of their IT needs ('workloads') from their own managed equipment ('on-premises') to the cloud, and in particular to public-cloud services that are shared between multiple business customers. This transition to the cloud supports the European Union (EU)'s 'digital agenda', which prioritises connectivity and cloud adoption to drive digital transformation.

Cloud services rely on customers being able to interact with the cloud platform, through the internet or a more direct connection. This close link with connectivity and a sense that a new paradigm around digital infrastructure is important to Europe's strategic autonomy and digital sovereignty, has led the European Commission (EC) to introduce the concept of 'collaborative connected computing', and to posit that cloud services and connectivity are 'converging'.

Some European policy makers and regulators, including the EC and BEREC, the group of telecoms national regulatory authorities (NRAs), appear to be considering whether and how to extend telecoms regulation to the cloud sector. Their positions are different:

- The EC's recent white paper, "How to master Europe's digital infrastructure needs?",[1] mentions the perceived need for a 'level playing field'[2] in regulation between cloud and connectivity, and asks whether the telecoms regulatory framework (in particular the European electronic communications code, or EECC) should be expanded to include cloud services.[3]

- BEREC's position is narrower, aimed at ensuring that the regulation of electronic communications networks and services as currently defined remains suitable in the context of further cloud adoption, specifically in the telecoms sector.[4]

In part, these positions reflect the stakeholders' broader interest in stimulating the digital agenda for Europe. However, the nature of this supposed 'convergence' between cloud and telecoms is often not well articulated and the rationale of the appeal for regulatory convergence is therefore not justified. These issues risk leading to unnecessary and counterproductive regulatory efforts, to the detriment of European consumers and businesses.

---

1 European Commission (2024), *How to master Europe's digital infrastructure needs?* (Brussels, 2024, COM(2024) 81 final); European Commission (accessed July 2024), *Europe's Digital Decade*.

2 See European Commission (2024), *How to master Europe's digital infrastructure needs?*, in particular p36.

3 This view that the distinction between cloud and telecoms is shrinking was made explicit by Roberto Viola, Director General for DG CNECT, speaking at the BEREC Stakeholder Forum in March 2024, where he was reported to have said that "no distinction between a cloud operator and a telecoms operator" and that therefore there cannot be a regulatory difference.

4 See BEREC (2024), *Draft BEREC Report on Cloud and Edge Computing Services*.

In this paper, we examine these questions in detail. In doing so, we draw on technical, legal and economic perspectives, considering the history of the telecoms sector and the purpose for which the telecoms regulatory framework was constructed and implemented.

2 Cloud and telecoms are distinct and complementary enablers of Europe's digital transformation

This section provides a brief introduction to the cloud, describing the role and benefits of cloud services, focusing particularly on public-cloud services. We then describe the cloud value chain and how different parts of the cloud ecosystem interact, examining how cloud services are delivered by different types of suppliers in the cloud sector. Finally, we explore the relationship between cloud and telecoms within the cloud sector, noting that cloud services are dependent on connectivity, and the slow pace at which telecoms operators are adopting public-cloud services for their network functions, through a combination of private- and multi-cloud architectures.

2.1 Cloud services enable European businesses to access scalable, globally competitive and state-of-the-art IT infrastructure and platforms, with limited investment and risk

Cloud services include a range of approaches to run software on distributed infrastructure. Public-cloud services are the focus of this paper: they are IT resources, or 'building blocks', shared between many business users and accessible through the internet. They offer significant economies of scale and a very 'elastic', or scalable, infrastructure. This allows businesses to access the IT infrastructure they require when they require it, paying as they go for the use of resources as opposed to having to invest heavily in their own IT infrastructure. As the cloud infrastructure and the software building blocks it supports are upgraded continuously, customers always have access to state-of-the-art services.

To maximise the benefits of scale enabled by a pooled use of IT resources, cloud services are global, and are 'horizontal' i.e. industry neutral in nature. They are typically accessed via application programming interfaces (APIs). Software that runs on cloud infrastructure includes cloud providers' services delivered through common APIs, and software developed by third parties including cloud customers themselves and other developers (independent software vendors or ISVs).

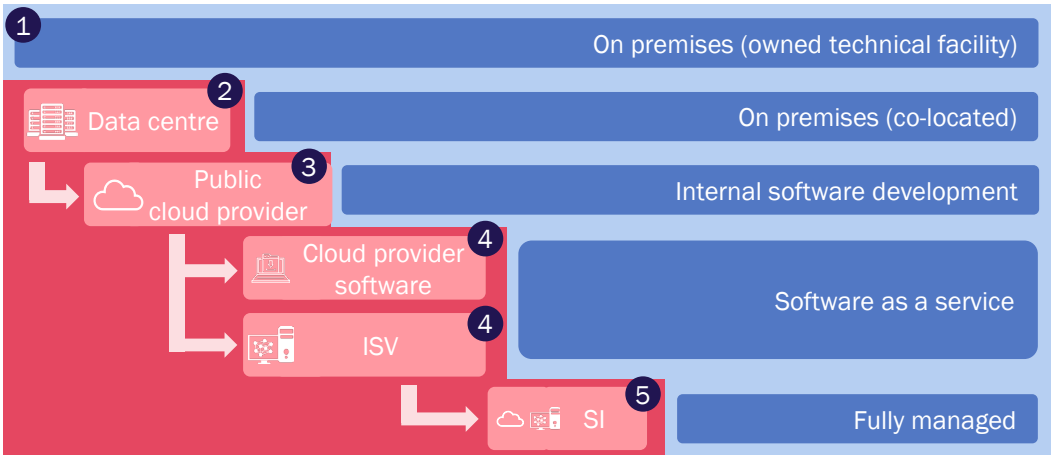
Cloud services offered by cloud providers are primarily used by businesses, not consumers. This contrasts with telecoms, where public electronic communication services are offered to both consumers and businesses, with most end users on the consumer side. While both sectors benefit from economies of scale and scope, they differ markedly in terms of network effects, through which end users benefit from being connected to the most widely used network. Historically, direct network effects in messaging and telephony were important factors governing the development of competition in the telecoms sector, whereas in the cloud sector network effects are primarily indirect, for example through nascent software marketplaces.

2.2 Businesses and ISVs, including in the telecoms sector, build applications and services using cloud infrastructure and building blocks

Cloud services are part of a broader IT value chain, bringing together data centres, servers and other hardware, software and services, with a wide variety of suppliers at all stages of the value chain. Cloud customers have the option to access services across the value chain at every stage, choosing to 'self-supply' or to buy from suppliers as they see fit.

A simplified view of the cloud value chain is shown in Figure 1 below. In the full 'on-premises' model (1), businesses deploy and operate IT hardware and software in their own premises. Many businesses choose to deploy their own hardware and software in 'co-location' data centres, owned and operated by third parties (2). Businesses that choose to migrate to the cloud can, at a basic level, purchase these cloud services as an input to their own software development and IT operations (3). In practice, thousands of ISVs, independent from cloud providers, build their own software and solutions on top of cloud services, in addition to software provided by cloud providers. This is offered 'as a service' to businesses and consumers (4). Systems integrators (SI) bring together software and services to offer fully managed solutions to customers who require more support (5).

Figure 1: Components of the cloud value chain [Source: Analysys Mason, 2024]



In the telecoms sector, operators use cloud services in the same way as businesses in any other industry, including for customer care software, data analytics and artificial intelligence (AI). Network functions that control and manage end-user traffic remain primarily fully managed by operators on 'private clouds' and on-premises infrastructure. So far, estimates based on operator surveys suggest that less than 1% of telecoms network workloads run on the public cloud.[5] Indeed, where operators run network functions in the cloud, we understand this is primarily in private clouds, via ISVs, many of which are long-term vendors to telecoms operators (e.g. Nokia).

5 See BCG (2024), *How to Find the Right Balance in the Telco Cloud* and Analysys Mason (2024), *Network cloud infrastructure: worldwide forecast 2023–2028*.

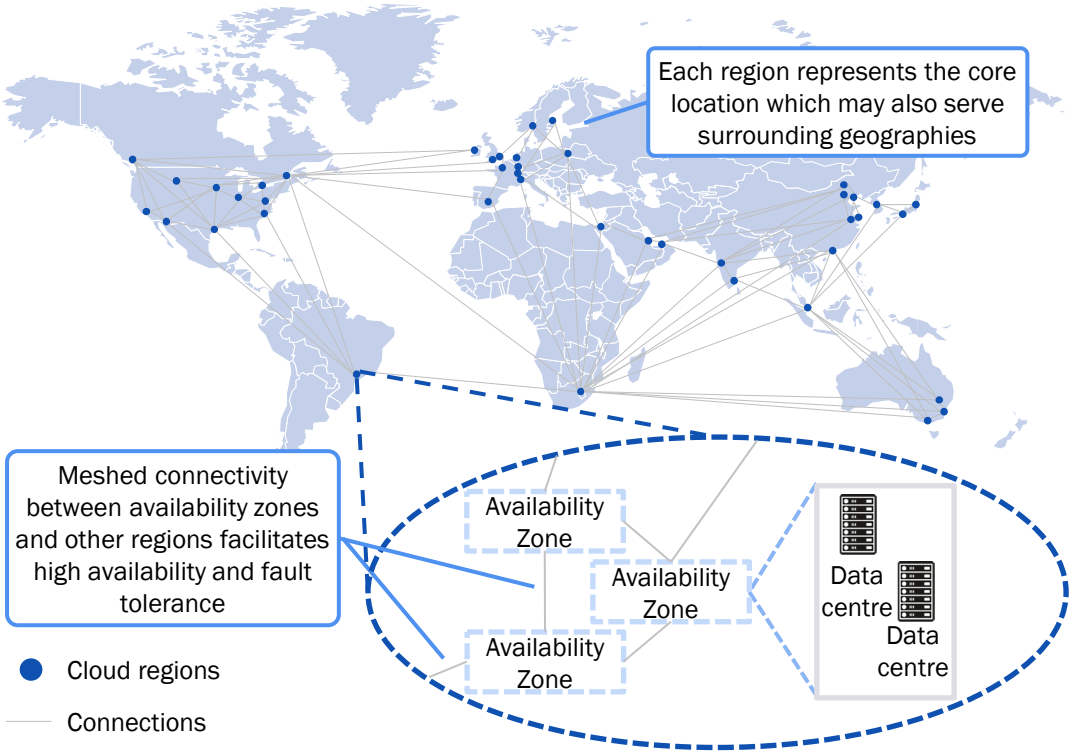
From the perspective of cloud providers, the telecoms sector is one of many customer segments, which they serve with a portfolio of 'horizontal' services that is available to all customers.

2.3 Cloud providers and cloud customers are dependent on connectivity, both as an input through private networks and for end users to access cloud services

Cloud services require connectivity, both for cloud providers to operate a distributed, scalable infrastructure, and for cloud customers to access their services. Typically, cloud providers operate in multiple, geographically distributed data centres. These must be connected to one another through high-capacity networks for the platform to function properly and deliver scale, elasticity and resilience. Such links are operated as a private network by cloud providers, which can lease links from telecoms operators or deploy their own by building out their own passive infrastructure including fibre cables depending on what makes economic and operational sense.

The resulting global infrastructure that characterises cloud platforms is illustrated in Figure 2 below.

Figure 2: Illustration of regions and availability zones [Source: Analysys Mason, 2024; this does not represent any specific cloud provider's deployment]



At the same time, cloud customers need to be able to reach their cloud provider to use its services. While they can do so directly through their own private network, they usually rely on an internet service provider (ISP) for connectivity through the internet or through dedicated connections (cloud 'on ramps'). This is similar to other internet-based services: customers of an online banking service must be able to access the service using their internet connection, and net neutrality regulation including the EU's Open Internet Regulation seek to ensure this is not blocked or degraded by ISPs.

Additionally, some cloud customers use content delivery networks (CDNs), which can store ('cache') and optimise the delivery of online content across the public internet. Some large content providers operate their own CDNs, and many businesses (including e-commerce platforms, European broadcasters, games publishers and other businesses with an online presence) use third-party CDNs from cloud providers and other specialised entities. These third-party CDNs handle content on behalf of CAPs, which are the ones that decide how and when to use CDNs and control the content that is delivered through them.[6] They deliver content to ISPs as close as possible to end users, optimising latency and costs for all parties.

These various ways in which telecoms and cloud interact have given rise to partnership opportunities, on which telecoms operators and cloud providers are actively collaborating. This suggests a complementarity between the cloud and telecoms sectors, but while at this stage cloud providers and customers are reliant on connectivity, by contrast telecoms operators are using public-cloud services in a limited way that largely excludes network functions. We note that telecoms operators can and do offer cloud services to business customers. These services are not regulated under the telecoms regulatory framework.

3 Major differences between the cloud and telecoms sectors undermine the application of the EU telecoms regulatory framework to cloud services

This section compares the dynamics at play in the telecoms and cloud sectors and assesses the rationale for regulatory convergence from an economic and legal perspective.

The key questions when considering regulating a sector of the economy are whether there is a market failure that needs to be addressed, and if so, how best to do so. In considering expanding the telecoms regulatory framework to cloud services, European policy makers and regulators therefore need, as a first step, to articulate the problem or market failure they are trying to solve. They should then consider whether recently introduced regulation applicable to cloud providers (e.g. the Data Act, Digital Markets Act, Digital Service Act, and regulations including NIST and NIST2) could effectively address these issues. Finally, if regulatory or competition concerns subsist, they should assess whether the purpose, history and mechanics of the telecoms regulatory framework in Europe are well adapted to remedying these problems, in a way that is consistent with the purpose of the telecoms regulatory framework, justified and proportionate.

3.1 EU telecoms regulation reflects the transition from state-owned monopolies to a vibrant private sector where competition and regulation interplay successfully

The EU telecoms regulatory framework was put in place to facilitate the evolution from state-owned national monopolies to an open, competitive sector. Extensive regulation was required to bring about

6 Examples of AWS CloudFront customers include broadcasters ProSiebenSat.1 in Germany and M6 in France, games publisher Rovio from Estonia, among many others.

this change, with certain regulatory measures remaining necessary and being enforced to this day to address the specific challenges inherent to the sector.

In the genesis of the telecoms framework, ex-ante regulatory intervention liberalised the market (i.e. allowed market entry) by addressing specific barriers to entry and by limiting the power of specific regulated actors (whose market power was partly derived from persistent structural features of the sector). In addition, ex-ante regulation dealt with defined policy objectives and consumer protection issues, based on a justified and proportionate approach that recognised the intrusiveness and potential negative impact of ex-ante regulation. Over time, the regulatory framework transitioned from a patchwork of national approaches to a broadly harmonised set of European rules, implemented nationally by national regulators, overseen by the EC.

To this day, the continued areas of focus for telecoms regulation remain influenced by this evolution. Market access is facilitated through the issuance of general authorisations. Regulators also administer the allocation of scarce resources, such as spectrum and telephone numbers. Some structural issues are persistent, linked to network effects, economies of scale and scope, and enduring competitive bottlenecks. In particular, the persistent market power of former state-owned incumbents is addressed through a mix of general authorisations and regulatory remedies imposed on any party with significant market power. These include mandated access to infrastructure and wholesale services, and the effective resolution of disputes regarding these issues. NRAs are constrained from imposing intrusive ex-ante remedies beyond the minimal conditions of general authorisation unless they have undertaken a detailed market analysis, in a process scrutinised by the EC.

The current version of the European framework recognises the progress made towards more effective competition, encouraging deregulation where possible while still allowing NRAs to impose additional rules, ex-ante only, subject to strict tests. The telecoms sector remains subject to general competition law, which continues to be the main recourse mechanism for other competition issues.

3.2 The EU telecoms regulatory framework responds to specific sector dynamics and policy objectives, which are very different to those in the cloud sector

The EECC framework is designed to address policy objectives within the specific dynamics of the telecoms sector. These dynamics resulted in incumbents benefitting from entrenched market power, due to:

- the maturity of demand in the telecoms sector: the vast majority of households and businesses had a fixed line before telecoms were liberalised
- persistently high barriers to entry and an inherent inability of end users to self-supply in all but niche cases, due to network effects and localised economies of scale
- direct network effects associated with telephony, where the ability to reach another user was at the heart of the nature of the service, benefitting large established network operators at the expense of new entrants.

In contrast, the cloud services sector exhibits rapid growth, which builds on businesses' existing demand for IT infrastructure and services. These needs have previously been self-supplied (i.e. through on-premises deployments). This has resulted in a sector in which cloud providers continue to compete for customers by encouraging new users away from self-supply towards cloud services. Other dynamics specific to the cloud sector also include the availability of inputs such as co-location data centres and computing capacity, which can be used by new entrants in the cloud sector to build their offering progressively. Additionally, direct network effects are not prevalent in the cloud sector, as one user's demand for cloud services is not affected by the number of other users using the same cloud service beyond economies of scale. These differences are summarised in Figure 3.

Figure 3: Summary of differences between the cloud and telecoms sectors in the context of the objectives of the telecoms regulatory framework [Source: Analysys Mason, 2024]

Area	Telecoms sector	Cloud sector
Market characteristics	Consumer and business-oriented sector. Stable and mature market structures stemming from a history of monopoly suppliers and no realistic prospect to self-supply.	Business-focused sector, with large enterprises making up the majority of current cloud spend.[7] Developing from a history where businesses self-supplied IT infrastructure and services, building on co-location data centres. Comparable but differentiated products and services offered by a range of cloud providers.
Innovation and investment	Reasonably slow innovation with new technologies developed and deployed over many years. Long payback periods with active equipment depreciated over 8–10 years and passive infrastructure much longer.	Fast-paced innovation with new technologies and services deployed continually. Short payback periods with servers depreciated over five years, enabling quick adoption of new developments.
Contestability by new entrants	Challenging given high barriers to entry including significant up-front investments in infrastructure required, and in some cases also access to scarce resources. Market maturity requires new entrants to compete for existing customers, which is made more difficult by the importance of direct network effects.	Growing sector, allowing new players to compete for customers taking cloud services for the first time. The 'incumbent' is primarily self-supply, including through private infrastructure. Greater contestability than telecoms, thanks to the wide range of models, including use of a 'virtual' model, the emergence of niche players (e.g. focusing on AI), and ability to scale investments as demand grows.
Competition	High standardisation of services resulting in commoditisation and	High levels of innovation to enhance user experience resulting

7 See for example CMA (2024), *Public cloud infrastructure services market investigation, Updated issues statement, 6 June 2024*, paragraph 7: "the top 10% of customers account for a very large majority of revenues and the top 1% account for over half of revenues".

Area	Telecoms sector	Cloud sector
	relative ease in switching which supports competition for existing telecoms users. Limited use of multiple providers for a given service, partly due to interoperability limitations and to procurement considerations. Resulting 'access monopoly' to a given customer at a given point in time.	in differentiation between providers. Provider differentiation could lead to interoperability challenges/barriers to switching which has the potential to reduce competition for existing cloud users. Wider use of 'multi-cloud' and hybrid cloud with allocation of workloads (i.e. subset of customer demand) to best application.
Network effects	High network effects due to need to connect two users trying to communicate, meaning that, unless there is interconnection, networks with larger user bases would have an advantage.	No direct network effects as the value of a cloud platform to a user is not dependent on other users.

Regulations specific to the telecoms sector, in particular focusing on interconnection and access to network facilities, were deployed to address barriers to entry and competition issues that arose under the telecoms market structure. The differences between the telecoms and public-cloud sectors shown in the table above clearly demonstrate that these regulations are neither necessary nor proportionate for the public-cloud sector.

Various competition authorities in Europe (including the UK) have in recent years conducted assessments of the cloud sector, which have highlighted several potential issues relating to competition. Despite these investigations, no regulatory interventions have been implemented to date. Importantly, the potential issues identified are distinct from those present in the telecoms sector, or stem from the fundamentally different dynamics between the two sectors. Therefore, applying the EECC would not be proportionate or effective in addressing these concerns.

Furthermore, the cloud sector is already regulated through a range of general and sector-specific regulatory tools at the EU level, which competition authorities recognise may address some of the potential issues identified. These include several new regulations related directly to digital markets, including the Digital Markets Act, Digital Services Act and Data Act, as well as directives such as NIS2. These are still being implemented and their effects have not yet been assessed fully.

Finally, we note that cloud services used by telecoms operators are treated in a similar way to network equipment provided by vendors including Nokia, Ericsson and others. These services and equipment are outside the scope of the EECC, but are constrained by regulatory obligation that apply to telecoms operators and affect suppliers through contractual means. For example, equipment and cloud vendors must comply with a range of requirements related to security, risk assessment and risk mitigation as part of services they may supply to telecoms operators. Policy makers also have

the ability to restrict telecoms operators from using vendors deemed 'high risk', through the EU toolbox for 5G security and national measures.[8]

3.3 Networking-related cloud inputs and products do not exhibit characteristics that would make them susceptible to regulatory alignment with telecoms regulation

As developed above, cloud services are not a substitute for electronic communications services and connectivity more generally. There is no 'convergence' between telecoms and cloud services, but rather a complementarity, where cloud services rely on the ability of cloud providers and customers to reach one another through the public internet or other network inputs.

Cloud providers make use of an array of such network inputs including private networks, and exchange of IP traffic (sometimes called IP interconnection) with ISPs and CDNs to enable end users to access content and applications in the cloud. None of these aspects have been found to be subject to specific market failures or competitive issues:

- BEREC has recently found[9] that IP interconnection on the internet has worked well and continues to do so, in the absence of regulation. This is in part reflected in the lack of any significant disputes related to IP interconnection between cloud providers and ISPs in Europe. BEREC found that IP interconnection has worked well, developing in a way that has enabled the internet to grow and thrive and supporting significant increases in demand without large increases in costs.

- Cloud providers' private networks enable connectivity between their data centres and points of presence (PoPs). In some instances, cloud providers directly invest in fibre networks for this purpose (including investments in submarine cables) as a substitute for purchasing capacity. However, capacity is never provided directly to end users or sold on to third parties through wholesale agreements, but only used for private network links supporting cloud services.

- CDNs primarily involve the decentralised storage and distribution of online content. They are used by content providers to improve their customers' experience, and help minimise the costs associated with increasing internet traffic. CDNs do not deliver traffic or services directly to end users, which is always the responsibility of an end user's ISP. The same BEREC report has found that CDNs play an important role in enabling the internet to scale.

Overall, this suggests there are no specific characteristics of cloud services that would justify deviation from the current regulatory treatment of IP interconnection, private network or CDNs. In practice, the EECC would be ill-suited to regulate these areas, even if there were issues.

8 European Commission (2020), *EU toolbox for 5G security*.

9 BEREC (2024), *Draft BEREC Report on the IP Interconnection ecosystem*.

IP interconnection between cloud providers and ISPs, or between CDNs and ISPs, is essential to end users' ability to access cloud services. Cloud providers and customers are entirely dependent on the ability to exchange traffic with one another for the service to work.

This type of interconnection is different from the EECC's definition of interconnection, which focuses on traditional telephony. The telecoms regulatory framework specifies interconnection rules, and indeed relevant interconnection markets were regulated for many years, to address specific challenges related to the importance of direct network effects in telephony: incumbents and other large operators had a strong incentive to refuse to interconnect with new entrants, or to make it very expensive, to discourage end users from switching operators.

This concern is not relevant to cloud services, where direct network effects are not prevalent, and services are provided 'over the top'. Market failures related to direct network effects are therefore not a significant risk, because cloud customers do not benefit directly from a cloud provider having more customers, beyond economies of scale. This undermines the relevance of the EECC's regulation of interconnection for ECS providers, which is designed specifically to remedy potential market failures associated with direct network effects in telephony.[10]

4 Extending telecoms regulation to cloud services risks harming Europe's consumers, businesses and digital agenda

In this section, we provide initial thoughts on the potential consequences of bringing cloud services under the telecoms regulatory framework. We consider the impact this could have on cloud providers and their customers, telecoms operators and their own customers, and the broader digital agenda for Europe.[11]

From this assessment, we believe it is likely that these effects would be counterproductive to the digital agenda for Europe, negatively affecting European businesses that use cloud services and CDNs, slowing down the adoption of cutting-edge technology that runs on cloud, including AI, and distorting competition in the telecoms sector. Finally, expanding existing telecoms regulation to a new sector, with no clear justification or impact assessment, would go against the EU's established principles and would materially increase regulatory risk and affect investor sentiment.

10 Note that the transition to IP telephony did not solve this problem directly, in a market environment where managed voice over IP was still subject to traditional voice call termination bottleneck. The move to interpersonal communications services provided over the top, without an operator needing to be involved, reduced this issue in the telecoms sector, displacing it to these interpersonal communications services. While the EECC does not specifically address interoperability between these services, the Digital Services Act, which already governs cloud services, does cover this aspect.

11 The digital agenda aims to increase take-up of cloud services so that 75% of EU companies are using "cloud, AI, or Big Data", ensure 90% of SMEs reach a basic level of digital intensity, and double the number of successful 'unicorns' valued at over EUR1 billion (or USD1 billion).

4.1 Expanding the telecoms regulatory framework to include cloud and CDN providers would directly affect their costs and incentives to invest in Europe

If the European telecoms regulatory framework were expanded to include cloud and CDN services, providers of these services would face additional cost, complexity and risks in operating in Europe. This could discourage further investment, and result in infrastructure (both cloud regions and PoPs) that becomes more centralised once again, in larger cities and countries. Smaller Member States could be most affected, as demand for cloud and CDNs may be insufficient to justify providers being regulated in additional (and in particular smaller) Member States.

Compliance costs and complexity associated with national regulation

The EECC is a directive that is implemented and enforced in each Member State, by different NRAs, in different ways. This is aligned with the national history and scope of the telecoms sector, and the localised economies of scope and scale that characterise it. It is at odds, however, with the global and cross-border nature and economies of scale of the cloud and CDNs, which has been recognised via the EU-wide scope of the Data Act and the Digital Markets Act for example.

Large cloud and CDN providers may be better equipped to deal with the complexity and costs associated with regulation. However, they would also be most affected by the risk of fragmented national regulations, compared to smaller providers that may be present in fewer Member States.

Higher costs related to IP interconnection

The inclusion of cloud and CDN providers under the EECC could result in IP interconnection between these providers and ISPs becoming regulated. This would be a significant departure from the successful approach of negotiated interconnection that has allowed the internet to grow rapidly, with increasingly decentralised infrastructure and interconnection.

In the context of strong lobbying by large telecoms operators to mandate and regulate interconnection with large content and application providers (CAPs), including cloud and CDN providers, this could lead to an increase in disputes that NRAs would have to arbitrate. This is a complex, time-consuming and costly process, which does not respond to a clearly established problem: indeed, BEREC and others have clearly said they view IP interconnection as a well-functioning part of the internet.

Complexity and costs associated with the regulation of private networks and CDNs

Similar cost, complexity and uncertainty would stem from the inclusion of cloud and CDN providers' private networks under the EECC. Third-party CDNs are intermediary services that act on behalf of CAPs. These CAPs control the traffic that is delivered through CDNs, and technical aspects related to the encoding, compression and access controls associated with the content itself.

Furthermore, the purpose and construction of the EECC have very clearly distinguished between public ECSs and public electronic communication networks (ECNs), which it oversees, and private networks, which are in summary not subject to regulation.

Bringing CDNs and private networks of cloud providers within the scope of telecoms regulation risks bringing private networks more generally under the regulatory framework and increase costs for the European businesses and CAPs that rely on cloud and CDNs, with no clearly articulated rationale or market failure.

Ultimately, the European businesses that use cloud and CDNs (including European CAPs) would likely face higher costs and lower-quality services as a result.

4.2 The impact on the telecoms sector would also be broadly negative, for most operators, for consumers and for regulators

If cloud and CDN providers faced higher costs and adverse incentives related to their investment in infrastructure in the EU, this could affect the telecoms sector through higher costs and investment requirements, reduced competition and poorer competitive outcomes, including for consumers.

More centralised interconnection could increase costs for telecoms operators

If cloud and CDN providers were present in fewer cities and countries across the EU, many European telecoms operators would have to expand their own network capacity to major peering locations, or purchase more capacity from large transit providers.

In addition, if cloud and CDN providers were included under the scope of the EECC, they may have fewer incentives to partner with ISPs/telecoms operators (e.g. for cloud on-ramps). They could also choose to operate submarine cable landing stations themselves, without partnering with telecoms operators.

Smaller ISPs may be disadvantaged compared to larger ones

If large ISPs were successful in extracting IP 'termination charges' from cloud and CDN providers that are above their costs, they would benefit at the expense of smaller ISPs, because their scale would result in greater transfers of funds from cloud and CDN providers. This would recreate the historical issue with fixed and mobile termination rates, which NRAs and the EC spent over 20 years solving, and risks distorting competition in the telecoms sector to the benefit of larger operators.

Competitive imbalances could result in larger operators self-

If a regulated termination monopoly for individual ISPs' end users resulted from these changes, new issues may emerge. For example, the largest operators may offer their own CDN services to CAPs and enterprise users, leveraging their larger networks to favour their own services. This would

preferencing their own cloud and CDN services	recreate the harms that existed in traditional call termination markets, and would go against European policy efforts to reduce self-preferencing in digital markets, including through the Digital Markets Act.

These negative effects on operators have been widely acknowledged by competitive operators.[12] Some larger incumbent operators also appear to recognise these risks, particularly in the context of CDNs.[13] They play an important role in the internet's ability to accommodate growing consumer demand without commensurate increases in costs, which could be put at risk by expanding the telecoms regulatory framework without a strong justification and impact assessment.

4.3 These impacts would be detrimental to European businesses on their digital transformation journey, the digital agenda and the ability of the EU to innovate through technology

We acknowledge that the discussion in the EC's white paper is preliminary and as such remains very superficial. However, early responses to the consultation suggest there is significant concern from multiple stakeholders around these proposals. Furthermore, the EC's perspective as outlined in the white paper is primarily focused on the supply side, and does not yet address the impact on the demand side, which is critical for a comprehensive impact assessment.

The positions shared by stakeholders in response to the consultation on the EC's white paper reflect the breadth of negative impacts that would stem from this proposal. In addition to negative impacts on cloud and CDN providers, and on smaller telecoms operators (discussed above), European businesses would face higher costs for cloud and CDN services. The impact of higher costs, including for IP interconnection, will ultimately be borne by end users, including European businesses and content providers, and by consumers.[14]

This could slow the deployment of some services in the EU, and slow adoption of cloud services and innovations, more broadly, including AI. This would be clearly counterproductive to the EC's efforts to spur digital transformation under its digital agenda. Ultimately, this would come at a cost for European competitiveness.

Other counterproductive effects would stem from more centralised digital infrastructure, and reduced investment in the EU. This would be the consequence of the risk of fragmented national

---

12 Ecta (2024), *Ecta considerations on the EUROPEAN COMMISSION'S WHITE PAPER "HOW TO MASTER EUROPE'S DIGITAL INFRASTRUCTURE NEEDS?"*.

13 See for example BEREC, BEREC (2024), *Draft BEREC Report on the IP Interconnection ecosystem*, (Section 4.5: "Technological developments, such as the installation of on-net CDNs, are a key reason why increases in data traffic have not passed through to prices and costs") and ETNO and GSMA (2023), *Summary of the Joint Telecom Industry Response* ("Intermediaries like commercial content delivery networks (CDNs) should not be considered [as 'large traffic generators' or] LTGs, but the traffic conveyed via such intermediaries should count toward the LTG designation threshold."

14 See BEREC (2022), *BEREC preliminary assessment of the underlying assumptions of payments from large CAPs to ISPs*: "Payment disputes between ISPs and CAPs can result in a loss of quality of the connection (as for example the dispute between Comcast and Netflix in the US demonstrated). To whom ISPs' customers attribute this problem and whether they are more likely either to switch the ISP or to switch or unsubscribe from the CAP, shapes the extent to which ISPs can exploit excessive charges, **which are ultimately paid by consumers**." (emphasis added)

regulation, centralisation of cloud regions and IP interconnection points in fewer jurisdictions, or even outside the EU, and less collaboration between cloud providers and telecoms operators, including on submarine cables and cloud on-ramps.

Finally, and perhaps most importantly, the EC's apparent proposal to repurpose a successful, complex regulatory framework designed for the specific characteristics of telecoms, to apply them to a very different sector, risks fundamentally undermining regulatory certainty. European policy makers need to ensure that any new regulation on cloud and CDN providers responds to a clearly established problem or market failure, which cannot be remedied through existing instruments, in a proportionate way. These principles are at the core of the telecoms regulatory framework and should be preserved.

5 Conclusions

Any argument for extending the telecoms regulatory framework to cloud services requires scrutiny based on the EU principles of necessity and proportionality. The telecoms framework, embedded in the EECC and enforced by NRAs, addresses a history of national monopolies and persistent high entry barriers in the telecoms sector. It has successfully promoted market entry, build-out of advanced connectivity, and competitive pricing.

Cloud services, however, differ fundamentally from telecoms networks. They are nascent, dynamic, global, and lack direct network effects, whereas the telecoms sector is mature, stable, location specific, with significant direct network effects. The telecoms regulatory framework, designed for a different history, sector dynamics and set of services, is not suited to regulating the cloud sector. The cloud sector is already overseen through European competition law, and is subject to newly introduced regulations that are all outside the telecoms regulatory framework. If competition or regulatory concerns subsist despite these regulations and guardrails after they are fully implemented, regulators should seek to remedy them through proportionate and justified remedies.

Applying telecoms regulation to cloud services could stifle growth and competition, disrupt the competitive balance among telecoms operators, incur higher costs for cloud users, and reduce choice and quality of services for users in both sectors. It could also hinder key EU initiatives such as Europe's digital decade and the Digital Single Market, while disproportionately affecting smaller providers and users across the ecosystem.

Both the cloud and telecoms sectors are vital for European digitalisation and competitiveness. Regulators should acknowledge the potential adverse impacts of extending the telecoms framework to cloud services and adopt a nuanced approach that recognises the unique characteristics of both sectors to support continued growth and innovation.