analysys mason

Final report for Amazon Web Services

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

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

This report is available in full 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.

0 Executive summary

0.1 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.

0.2 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.

0.2.1 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).

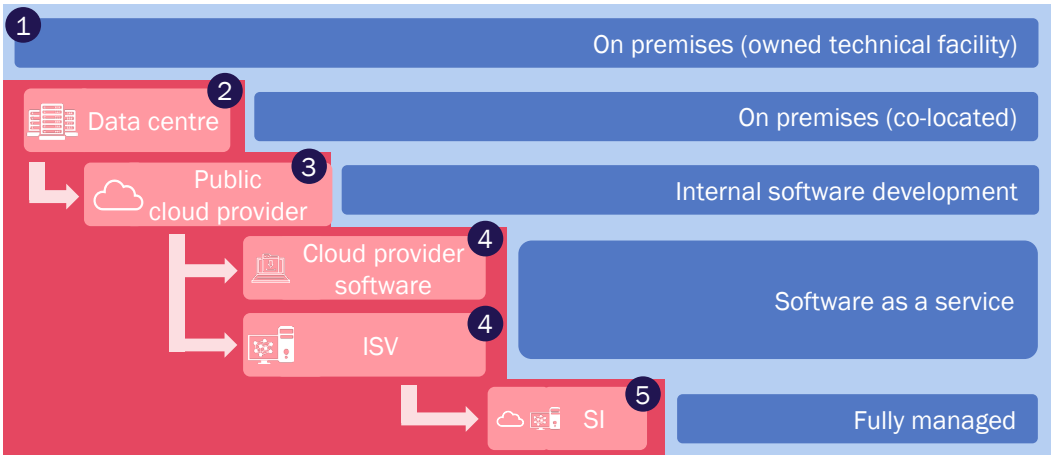
Cloud services offered by cloud providers are primarily used by businesses, not consumers. This contrasts with telecoms, where public electronic communication services are offered to both consumers and businesses, with most end users on the consumer side. While both sectors benefit from economies of 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.

0.2.2 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 0.1 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 0.1: 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*.

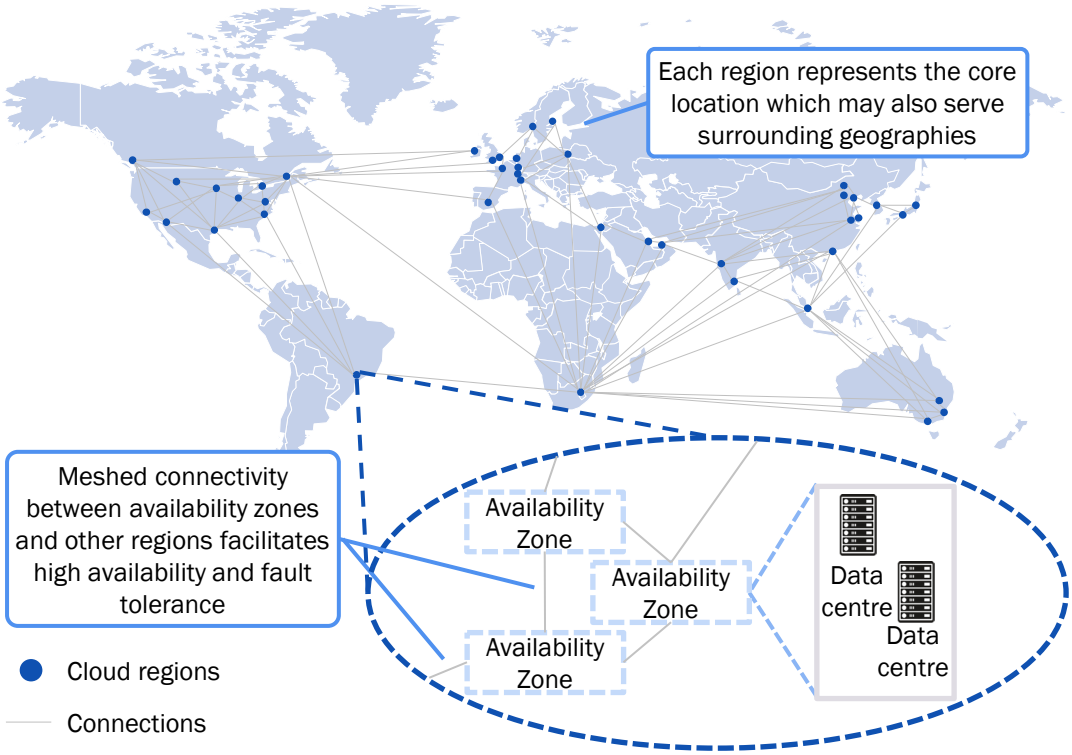
From the perspective of cloud providers, the telecoms sector is one of many customer segments, which they serve with a portfolio of 'horizontal' services that is available to all customers.

0.2.3 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 0.2 below.

Figure 0.2: 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.

0.3 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.

0.3.1 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.

0.3.2 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 0.3.

Figure 0.3: 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]

0.3.3 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]

0.4 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).

0.4.1 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.

0.4.2 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.

0.4.3 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.

0.5 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.

1 Introduction

Businesses are progressively adopting cloud services to meet their information technology (IT) needs, in addition to, or as a replacement for, functions performed with their own IT equipment. This shift from 'on-premises' private IT to 'public'-cloud services where infrastructure and systems are shared between multiple businesses, goes hand in hand with the increasing use of IT for automation, driven by sophisticated use of large volumes of enterprise data, including through artificial intelligence (AI). Cloud services have also enabled 'digital-first' businesses to launch and grow globally without the capital expense and risk associated with running their own data-centre infrastructure.

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'.

The EC discusses this concept in a white paper[15] that should help inform the EC's future policy and regulation related to the digital infrastructure pillar of its Digital Decade Policy Programme 2030. The white paper specifically mentions the perceived need for a 'level playing field'[16] 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.[17]

Part of the EC's rationale relies on a view that cloud providers are currently exempt from telecoms regulation (including access and interconnection), although they operate large backbone networks and 'interconnect' with regulated telecoms operators. This goes further than the conclusions BEREC draws from its own analysis of possible convergence between cloud and telecoms,[18] which focuses on ensuring that the regulation of electronic communications networks and services as currently defined remains suitable in the context of further cloud adoption.

While the idea of simply extending the current telecoms regulatory framework to cloud providers may seem appealing on the surface, this approach fails to acknowledge the fundamental differences between the cloud and telecoms sectors. It also overlooks the potential risks and costs associated

15 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*.

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

17 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.

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

with applying regulatory solutions, originally designed to tackle specific issues in the telecoms sector, to the cloud sector, which does not face the same issues due to its structure and characteristics.

In this paper, we examine these questions in detail, drawing on technical, legal, economic and regulatory perspectives, as well as historical context and analysis:

- Section 2 provides an introduction to the role of cloud services in the European digital economy, the value chain of cloud (including where it is used for telecoms) and the interactions between cloud and telecoms, which are sometimes inputs to one another, and in most cases complements, for the businesses and consumers that use cloud services.

- Section 3 reviews the current telecoms framework and the structural problems addressed through the imposition of specific ex-ante[19] rules across the telecoms regulatory framework, contrasting the dynamics at play in cloud and telecoms to assess whether similar problems exist in cloud. Finally, we also examine in more detail specific networking aspects of cloud: private network including submarine cables, IP interconnection between cloud providers and internet services providers (ISPs), and content delivery networks (CDNs).

- Section 4 explores the potentially negative impacts on the European Union (EU)'s Digital Agenda 2030, Europe's businesses, consumers, and the region's competitiveness, of extending existing ex-ante telecoms rules to the cloud sector.

- Section 5 summarises our main conclusions.

The analysis is supplemented by background information, historical context and legal references, included as annexes.

We have included summaries of key points at the start of each section, in a blue box such as this one.

19 These are rules that can be applied to prevent the abuse of dominant position, in contrast with ex-post competition law that applies when an abuse has taken place.

Acronyms used in this paper

Acronym	Meaning
ACM	Authority for Consumers and Markets (Netherlands)
AI	Artificial intelligence
API	Application programming interface
AWS	Amazon Web Services
BEREC	Body of European Regulators for Electronic Communications
CAP	Content and application provider
CDN	Content delivery network
CMA	Competition and Market Authority (UK)
DGA	Data Governance Act
DMA	Digital Markets Act
DSA	Digital Services Act
EC	European Commission
EECC	European Electronic Communications Code
ECS	Electronic communication service
ECN	Electronic communication network
EU	European Union
GDPR	General Data Protection Regulation
HHI	Herfindahl-Hirschman index
ISP	Internet service provider
ISS	Information society services
ISV	Independent software vendor
IT	Information technology
IXP	Internet exchange point
MTR	Mobile termination rate
NRA	National regulatory authority
NIS	Network and information systems
ONP	Open network provision
PaaS	Platform as a service
PoP	Point of presence
QoS	Quality of service
R&D	Research and development
SI	Systems integrator
SME	Small and medium-sized enterprise
SMP	Significant market power
VLOP	Very large online platform
WAN	Wide-area network

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

In this section, we discuss how cloud and telecoms are contributing to fulfilling the ambitions of the digital agenda for Europe and the EU's Digital Decade.[20] In Section 2.1, we describe the role of cloud services for European businesses, and the benefits they bring. In Section 2.2, we describe the cloud value chain and how different parts of the cloud ecosystem interact, examining how cloud services are delivered to telecoms operators by different types of suppliers in the cloud sector. Finally, in Section 2.3 we explore the relationship between cloud and telecoms within the cloud sector.

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

Summary

Cloud services allow businesses to run software using IT infrastructure and software 'building blocks'[21] that are shared with many other users, offering large economies of scale and a very 'elastic', or scalable, infrastructure.

This infrastructure, and the building blocks it supports, are upgraded continuously, ensuring that customers can access state-of-the-art services. Cloud services are 'horizontal' in nature, offering common functionalities to cloud customers in any industry and sector, typically through application programming interfaces (APIs). Software that runs on cloud infrastructure includes cloud customers' own software, and third-party software from a wide range of vendors, which can all use the same APIs.[22]

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.[23]

Both sectors benefit from economies of scale and scope. Historically, direct network effects in messaging and telephony were important factors governing competition in the telecoms sector, whereas in the cloud sector network effects are primarily indirect, for example through nascent software marketplaces.

20 See European Parliament (2024), *Digital agenda for Europe* and European Commission (accessed July 2024), *Europe's Digital Decade*.

21 These include data storage management, databases, 'containerisation' systems that allow physical resources to be used in software, AI tools and many others; these building blocks are sometimes referred to as 'platform as a service' (PaaS) tools.

22 AWS (2024), *What is an API? - Application Programming Interface Explained*.

23 The EECC Article 2(15) defines a consumer specifically as a natural person, accessing services outside a work context.

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

Summary

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. Cloud customers have the option to access services across the value chain at every stage, choosing to 'self-supply' or buy from suppliers as they see fit.

Businesses can choose to purchase these cloud services directly as an input to their own software development and IT operations. In practice, thousands of software vendors, independent from cloud providers, build their own software and solutions on top of cloud services. They then offer these 'as a service' to businesses and consumers.

In the telecoms sector, operators use cloud services in the same way as businesses in any other business sector. These include for example customer care software, data analytics and AI. Cloud-based networking, involving the control and handling of electronic communications signals by operators, remains limited. Some estimates from operator surveys suggest that less than 1% of network workloads[24] run on the public cloud. Cloud networking occurs primarily in private clouds, via independent software vendors (ISVs), many of which are long-term vendors to telecoms operators (e.g. Nokia).

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.

European businesses have access to a wide range of cloud infrastructure and platform services, which are offered by an array of cloud providers with varied profiles and backgrounds. Cloud providers offer infrastructure and software building blocks to ISVs and businesses that use these inputs to build cloud-based services. In the telecoms sector, operators use cloud services directly for their own software development needs, and in some limited instances as the platform on which to host 'cloudified' network functions provided by ISVs, primarily traditional telecoms equipment and solutions vendors such as Nokia and Ericsson.

2.2.1 Cloud services are part of a broader IT value chain in which 'on-premises' IT still plays a major role, supported by independent co-location data-centre providers

Cloud services are part of a broader IT value chain involving:

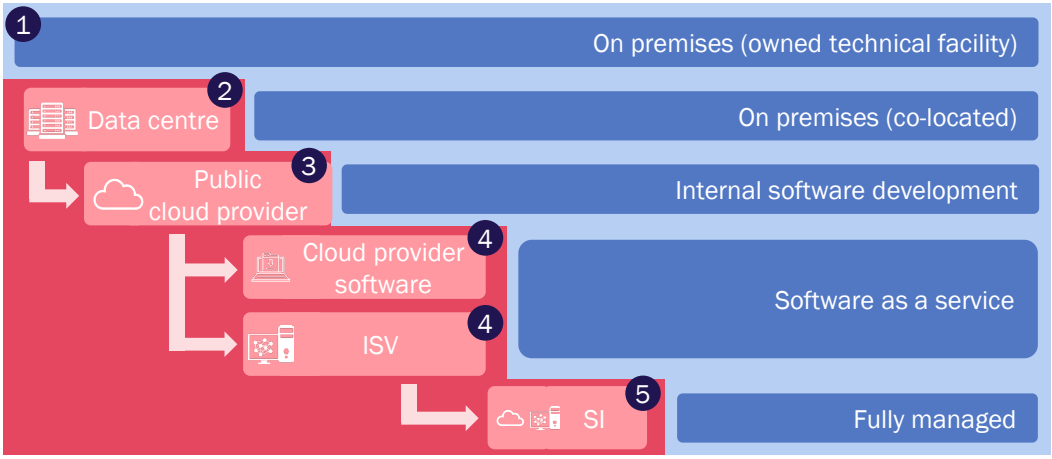
- physical infrastructure, primarily data centres (1)
- computing hardware and software building blocks (2)
- software applications and services (3)
- systems integrators (SIs) (4).

This value chain is accessible at all levels, leading to a range of models illustrated below in Figure 2.1. A simplified view of the cloud value chain is shown in Figure 0.1 below. In the full 'on-premises' model (number 1 in the diagram), businesses deploy and operate IT hardware and software

[24] A workload is a discrete unit of software running on IT infrastructure, including in the cloud.

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



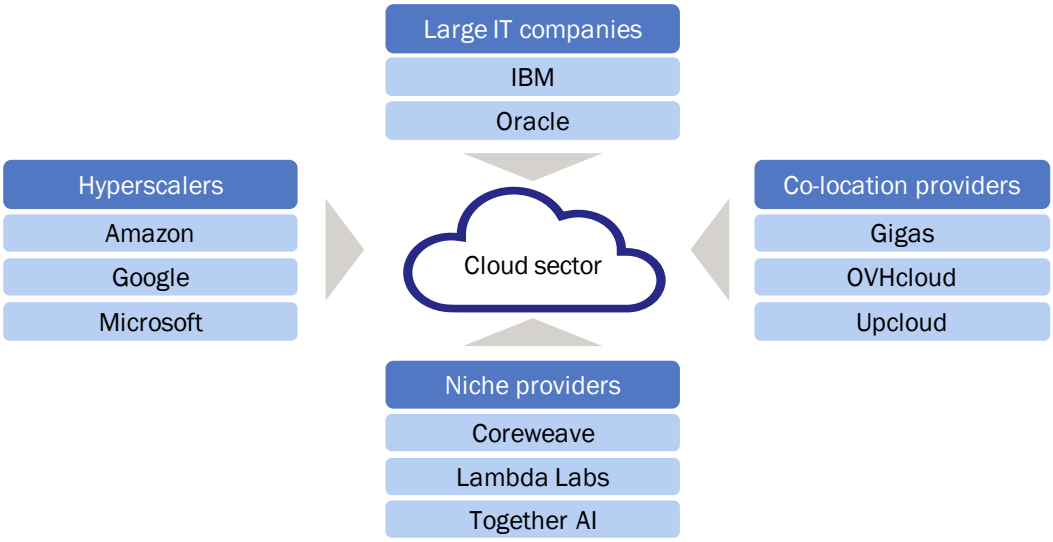
2.2.2 European businesses have access to a wide range of cloud infrastructure and platform services, offered by an array of providers with varied profiles and backgrounds

Numerous cloud providers have emerged from a variety of backgrounds and operate in Europe and worldwide. They cater to the diverse needs of European businesses by offering a wide range of services (see Figure 2.2):

- So-called 'hyperscalers', originating from businesses with large internal IT requirements, such as Amazon, Google and Microsoft, which they were able to repurpose to serve third parties.
- Enterprise IT service providers, such as Oracle and IBM, which have used their significant IT management capabilities to build cloud platforms to serve their existing customers.
- 'On-premises' co-location data-centre providers, such as OVHCloud, which have built on existing technical facilities to move up the value chain beyond passive co-location racks to owning and operating compute, storage and networking infrastructure.
- Smaller, more dynamic providers, which are emerging in response to customer demand for specialist capabilities in emerging technologies such as AI.

We note that at present, a small proportion of workloads are hosted on the public cloud, with the vast majority running in various 'on-premises' deployments, including 'private cloud'.[25]

Figure 2.2: Paths of entry to the cloud sector [Analysys Mason, 2024]



Telecoms operators are also entering the cloud space, with some building their own cloud platforms using existing large-scale IT infrastructure and IT managed services capabilities like hyperscalers and enterprise service providers. These include large operators such as Orange or Deutsche Telekom,[26] and smaller players such as Scaleway (part of Iliad Group).[27] Others are also partnering with other cloud providers to package and resell services to customers.

2.2.3 The cloud value chain brings together cloud providers that provide building blocks accessible through APIs, and ISVs and businesses that use these inputs to build cloud-based software

Both ISVs and individual businesses leverage the building blocks provided by cloud providers to develop their own software. ISVs develop software to be sold to other enterprises that may not have or need the IT capabilities to self-supply such solutions, often using a model known as 'software as a service'. Research by the Netherlands' Authority for Consumers and Markets shows the huge variety of products offered on major cloud platforms, the vast majority of which are provided by ISVs (see Figure 2.3).

25 A survey conducted by McKinsey, the results of which were published in April 2024, suggests that only 13% of cloud-using respondents had over 80% of workloads in the cloud, while 68% had fewer than 50%. See McKinsey & Company (2024), *The state of cloud computing in Europe*.

26 See Orange Business's *Cloud Infrastructure Solutions* and Deutsche Telekom's *Open Telekom Cloud*.

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

Figure 2.3: Number of products in own and third-party marketplaces by cloud provider [Source: Netherlands Authority for Consumers and Markets, 2022]

	Total number of products	Total number of first-party cloud products	Total number of ISV third-party products
AWS	12 591	408	12 183
Azure	18 046	304	17 742
Google Cloud	6276	92	6184

The ability of businesses to directly access basic building blocks on a flexible basis supports the development of cloud-native start-up and scale-up businesses without requiring them to invest in on-premises or private-cloud infrastructure during these early phases. Nearly all European technology companies use cloud services, including Spotify, Supercell and Deliveroo,[28] among many others.

The benefits of the cloud are relevant to ISVs more broadly, including established vendors that would have previously delivered software either through deployment on a customer's own infrastructure or via the internet from infrastructure owned by the ISV. By deploying software and services in the public cloud, ISVs are able to simplify the delivery of their services on a common infrastructure, and benefit from scalability as described above. ISVs that previously delivered services from their own infrastructure are also able to scale customers globally using the reach of public-cloud platforms, without the need to make infrastructure and hardware investments in new regions.

2.2.4 Like other businesses, telecoms operators use public-cloud platforms to improve their operations, and network vendors are offering products via the public cloud like other ISVs

Telecoms operators increasingly use the public cloud for a range of IT needs, but network cloudification is happening relatively slowly

Telecoms operators' IT requirement include network-related workloads, which are software functions that enable the provision of electronic communications services to their customers, and other IT needs including customer care, data analytics, billing, and other functions that are common to companies in many other sectors of the economy.

Like many other large businesses, telecoms operators are increasingly using public-cloud platforms to run software for operations, finance, customer service and business intelligence.[29] Worldwide spend by telecoms operators on OSS/BSS systems delivery is expected to increasingly shift towards the public cloud, reaching 27% of total spend by 2028 (i.e. USD21 billion), from 14% in 2023.[30]

28 See *Spotify Case Study*, *Supercell Case Study*, *Deliveroo on AWS: Case Studies, Videos, Innovator Stories*.

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

30 Analysys Mason (2023), *CSPs' spending on telecoms-related OSS/BSS software and services will reach USD80 billion by 2028*. CSP refers to communications service providers, which we term 'telecoms operators' more generally in this paper.

This shift is partly driven by ISVs' focus on public cloud-based solutions for telecoms, with some such as Amdocs[31] and Netcracker[32] partnering with cloud providers to offer services to telecoms operators.

Telecoms operators are also beginning to adopt cloud-based services for network functions, although this transition can be expected to be more gradual, given the historical vertical integration between software and telecoms hardware vendors and relatively long lifetimes of telecoms network assets that limit the speed of migration to cloud for existing telecoms networks.

Cloudified network functions are mostly deployed on private infrastructure, including private clouds, as telecoms operators seek to make use of existing owned data-centre facilities and retain greater control over these operationally critical assets. In some instances, telecoms operators and their ISVs may use parts of cloud providers' wider offerings – such as Telenet's use of Google Cloud's 'Anthos[33]' – whilst still operating a private-cloud model.

This is visible in available data and estimates. A BCG article from February 2024 suggests that, as of 2023, less than 1% of telecoms operators' network workloads are running in the public cloud.[34] Similarly, Analysys Mason's own research[35] estimates that only 2% of mobile network cloud spend by telecoms operators globally in 2023 was on public-cloud platforms, with forecasts that only 20% of total spend would be on the public cloud by 2028.

Where operators are deploying network functions in the public cloud, they do so through network equipment and software vendors operating as ISVs, drawing on horizontal cloud functions and APIs

There are some instances of new-entrant telecoms operators, which typically benefit from greater network deployment flexibility due to not being constrained by historical deployments, where network functions will be hosted in the public cloud such as DISH Networks[36] in the USA. Amongst the existing 'brownfield' telecoms operators (i.e. those with mature existing networks and operations), Telefónica Germany is the only one to have announced network function deployment in a public-cloud environment, initially at a relatively limited scale (the first phase targets 1 million users, around 2% of total subscribers).[37]

---

31 See Netcracker (2020), *Netcracker Delivers Digital Service Innovation with Amazon Web Services;* See Netcracker (2020), *Netcracker and Google Cloud Announce Strategic Partnership to Help Telcos Modernize Business and Operational Systems;* See Netcracker (2024), *Netcracker Successfully Implements Full-Stack, Cloud-Native BSS/OSS on AWS for Andorra Telecom*.

32 Amdocs (2024), *Finetwork Selects Amdocs to Modernize its Systems, Enabling Spanish Operator to Provide Fiber, TV and Mobile Services*.

33 Telenet, *Telenet introduces Ericsson, Nokia and Google Cloud as partners for the rollout of its 5G Network, the Engine for Future Mobile Innovation*.

34 BCG (2024), *How to Find the Right Balance in the Telco Cloud*.

35 Analysys Mason (2024), *Network cloud infrastructure: worldwide forecast 2023–2028*.

36 Nokia (2021), *Nokia and DISH to deploy first 5G standalone core network in the public cloud with AWS*.

37 Telefonica (2024), *First 5G core network in the cloud for an existing operator: O2 Telefónica sets new impulses in the core network together with Nokia and AWS*.

It is also worth noting that the deployment of network functions in the public cloud is based on a three-layer system, involving cloud providers, network vendors, and the operator itself.[38] In all announced uses of the public cloud for network deployments, the cloud provider acts only as the cloud infrastructure layer. This makes them a hosting platform on which ISVs, such as Nokia in the case of both DISH and Telefónica Germany, offer their services. Microsoft's 'Azure Operator 5G Core' was the first attempt by a major cloud player to offer core network services for telecoms operators directly, but recent announcements suggest that Microsoft will now revert to a 'horizontal' approach working with network ISVs.[39]

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

Summary

Cloud services require connectivity, both for cloud providers to operate a distributed, scalable infrastructure, and for cloud customers to access their services.

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. These links are operated as a private network by cloud providers, which can buy links from ECS providers or build their own links depending on what makes operational and financial sense.

Cloud customers need to be able to reach their cloud provider. They can do so directly through their own private network, but mostly rely on an ISP for connectivity through the internet or through dedicated connections ('on ramps'). Some cloud customers use CDNs, which can store ('cache') and optimise the delivery of online content across the public internet.

These various ways in which telecoms and cloud interact have given rise to partnership opportunities, which telecoms operators and cloud providers are actively collaborating on. This suggests a complementarity between the cloud and telecoms sectors, but at this stage cloud providers and customers are reliant on connectivity, whereas telecoms operators are using public-cloud services in a limited way, which largely excludes network functions.

In this section we explain how connectivity underpins cloud services:

- cloud providers use connectivity as part of their own infrastructure, to connect their data centres and PoPs across multiple locations
- cloud customers rely on connectivity to access cloud services, through the internet or through dedicated connections ('on ramps')
- CDNs are separate and complementary to cloud services, enabling online content to be cached and distributed efficiently close to end users.

38 Plum, Stratix for BEREC, *Study on the trends and cloudification, virtualization, and softwarization in telecommunications* (2023, BoR(23) 208).

39 See Microsoft, *Azure Operator 5G Core*, and LightReading (2024), *Layoffs crash into Microsoft's Azure for Operators*.

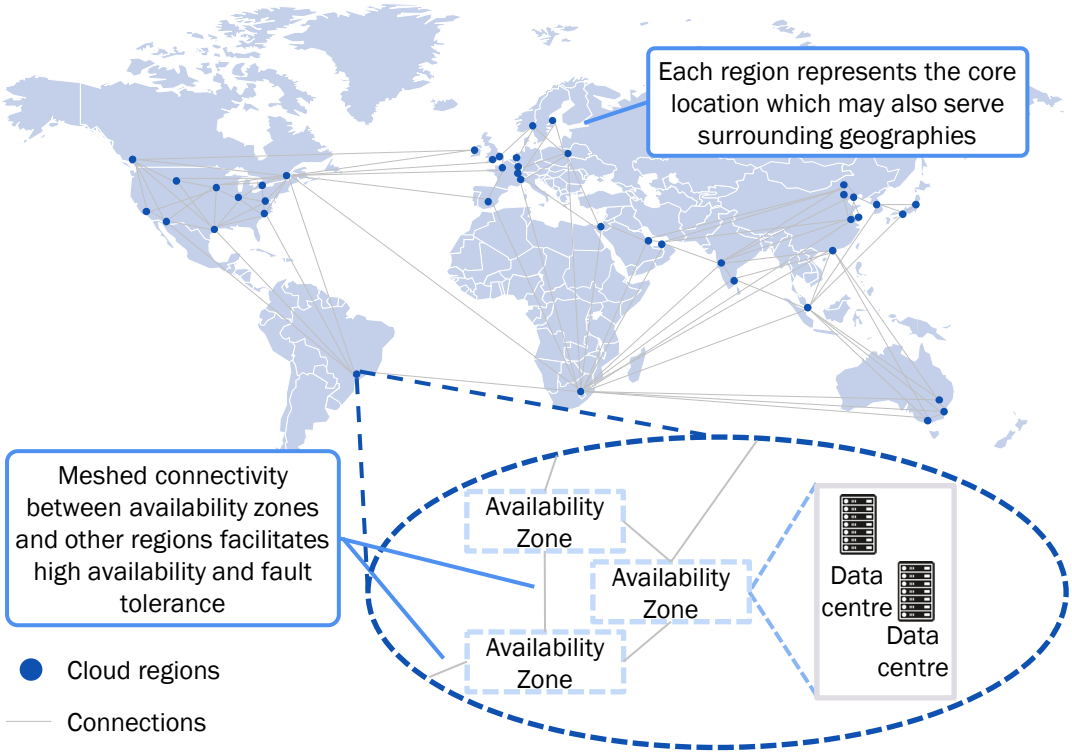
This forms the basis of the discussion in Section 3.3, focusing on the distinction between these three types of connectivity, and the electronic communication networks and services that are at the core of the European telecoms regulatory framework.

2.3.1 Cloud providers use domestic and international connectivity extensively as part of their operations, to connect their data centres and PoPs across the world

To offer their services, cloud providers deploy data centres worldwide in 'regions' and 'availability zones'. Regions are spread globally to best serve customers, comply with data sovereignty requirements, improve fault tolerance and provide disaster recovery capabilities. Each region is made up of multiple isolated data centres or availability zones[40] (themselves consisting of one or more isolated data centres), each with its independent power, cooling and networking infrastructure to further increase fault tolerance in the case of localised issues.

Cloud data centres and PoPs are connected through network links, as illustrated in Figure 2.4.

Figure 2.4: Illustrative global view of regions and availability zones [Source: Analysys Mason, 2024; this does not represent any specific cloud provider's deployment]



These links combine local, national and international connectivity. Connectivity between data centres in a given region, or between regions in a given country, is provided by a combination of

40 AWS availability zones are separated by up to ~100km; OVHCloud recently launched a new availability zone in Paris with data centres ~30km apart. Other leading cloud providers do not make similar details publicly available. See AWS (2024), *Availability zones* and Data Center Dynamics (2024), *OVHcloud launches multi-zone cloud region in Paris, France*.

dark fibre (on which the cloud provider operates its own networking equipment) and enterprise connectivity solutions from enterprise-focused telecoms operators.

The largest cloud providers are in some cases building their own network links, including through submarine cables, typically for very large capacity links between continents. In many such cases, cloud providers partner with telecoms operators, as part of consortiums and other partnership agreements that help both parties combine their expertise, share the costs of submarine cables, and benefit from the capacity created for their own use.[41]

Some cloud infrastructure is being deployed at the so-called 'edge', close to end users. In some cases, the edge is located within an ISP's network, through partnerships between major cloud providers and ISPs. This allows cloud customers to execute workloads closer to their premises, with reduced latency and transport requirements. Examples of such edge collaborations include Amazon Wavelength, which is currently offered by Vodafone in Germany and the UK,[42] and Google Anthos for Telecom which is partnering with AT&T in the USA.[43] At this point, edge nodes deployment remains limited, with the EC estimating around 500 edge nodes deployed at the end of 2022 throughout the EU, most of them seemingly unrelated to public-cloud providers so far.[44]

2.3.2 Cloud customers rely on connectivity to access cloud services, through the internet or through dedicated connections ('on ramps')

Cloud services are by nature 'online' services: they can only be used by customers who are able to reach the cloud platforms through some sort of electronic communication network and service. Cloud providers do not offer 'last-mile' connectivity (i.e. all the way to the end user) of any kind in Europe at the moment.[45]

Some cloud customers operate their own networks, and are able to connect directly with cloud providers through dedicated 'cloud on-ramp' services. Most cloud customers rely on an ISP to connect to their cloud services, either through the public internet or through an 'on-ramp' service provided by their ISP.

The quality of the connectivity provided by the ISP is important to the experience of cloud users, both in terms of latency and speed, and in terms of resilience and availability. Cloud providers and

41 TeleGeography (2024), *A (Refreshed) List of Content Providers' Submarine Cable Holdings*.

42 AWS, *AWS wavelength* (accessed July 2024).

43 Google (2020), *Bringing partner applications to the edge with Google Cloud.*

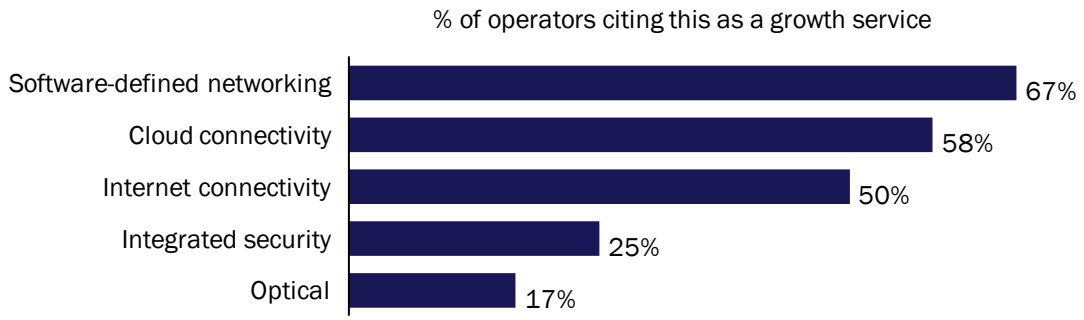
44 European Commission (2023), *Edge Observatory for the Digital Decade*.

45 We note BEREC's reference to mobile services provided by AWS and Google in the USA. It is worth noting that AWS Private 5G Radio is a private networking product 'in a box' using citizens broadband radio service (CBRS) spectrum, and that Google Fi is a mobile virtual network operator (MVNO) that, in the EU, would clearly be subject to the current telecoms regulatory framework. Neither of these products are currently available in the EU. See BEREC (2024), *Draft BEREC Report on Cloud and Edge Computing Services*.

telecoms operators work together through peering and transit relationships to achieve a high quality of service for their customers.[46]

The growing importance of cloud for enterprise users of connectivity is illustrated in a recent survey of ISPs, shown in Figure 2.5, which highlights the growing demand for software-defined services and cloud connectivity.

Figure 2.5: Fixed connectivity services cited by operators as delivering revenue growth[47] [Source: Analysys Mason, 2024]



The importance of connectivity as an enabler of cloud services for end users is evident in the digital transformation of businesses: as they adopt cloud services, they increase their demand for high-speed, reliable connections including new services such as on-ramps and multi-cloud networking. Conversely, as ISPs enhance their network infrastructure, it becomes easier and more attractive for businesses to adopt cloud services. This points to a degree of complementarity between cloud and telecoms services, although this remains asymmetric: cloud providers and customers both need access to connectivity as a critical enabler of cloud services, but telecoms operators do not rely on cloud services to offer connectivity.

2.3.3 CDNs are separate and complementary to cloud services, enabling online content to be cached and distributed efficiently close to end users

Some cloud customers who provide services to end users that are hosted on the cloud, including internet content and application providers (CAPs), use CDNs to optimise the delivery of their content across the internet. CDNs are complementary to cloud services but distinct, and the use of CDNs predates the broad availability of public-cloud services.[48]

---

46 For example the partnership between Telefónica and Oracle, offering B2B customers an on-ramp to Oracle Cloud infrastructure;
Deutsche Telekom and Microsoft cloud are partnering, targeting medium to large enterprises;
Telia connecting to AWS, Microsoft and Google in the USA, Europe and Asia.

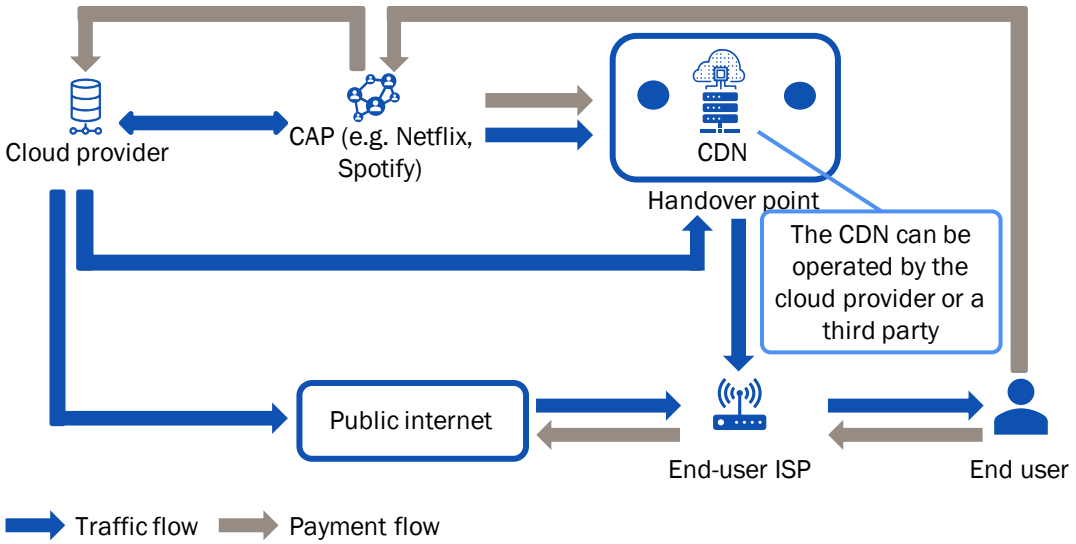
47 Based on responses from an unpublished Analysys Mason survey with 12 ISPs; while software-defined networking (SDN) is a networking technology and not a cloud access solution per se, in practice operators are using SDN to meet customer demands relating to increased cloud and Software-as-a-Service (SaaS) usage, such as hybrid and multi-cloud networking.

48 Akamai started offering CDN services in 1999, Akamai, *Company history (accessed July 2024)*.

CDNs use servers that store (or 'cache') content close to end users, sometimes within ISPs' premises ('on-net CDNs'). These cloud customers use a range of models, from different suppliers. Some large content providers operate their own CDNs (e.g. Netflix Open Connect[49] and Meta Network Appliances).[50] Most CDN users buy CDN services from third-party providers, including Akamai, Cloudflare, Fastly, and public-cloud providers including AWS, Microsoft and Google Cloud.

The mechanisms through which content flows on the internet have been described at length in previous papers, including from Analysys Mason[51] and recently in a BEREC paper.[52] Put simply, upon request of a specific piece of content by an end user, CDNs then serve the content from the cache that best optimises the quality of the user's experience, and the cost of delivering the content. In many cases, the content can be routed to the end user's ISP directly, avoiding the need for transit and optimising costs for the ISP, as illustrated in Figure 2.6. In a nutshell, using a CDN is the CAP's decision, and the cloud provider, CDN and ISPs are able to exchange traffic through peering relationships without having to manage commercial relationships and payment flows.

Figure 2.6: Traffic and payment flows in cloud networks with CDNs and CAPs [Analysys Mason, 2024]



Because of the benefits they bring to content providers, telecoms operators and end users, CDNs are now an essential component of the architecture of the internet. They are used extensively by broadcasters, streaming providers, online games companies and many other online CAPs. As a result, a significant share of internet traffic delivered to end users now goes through CDNs, as

49 See Meta, *Meta Network Appliances* and Netflix, *Open Connect* (accessed July 2024).

50 See Netflix, *Open Connect Overview*; Spotify (2020), *How Spotify Aligned CDN Services for a Lightning Fast Streaming Experience* and Google, *Spotify case study*; AWS, *ProSiebenSat.1 Media SE Delivers Interactive TV Experiences Using AWS Serverless Solutions.*

51 Analysys Mason (2024), *The impact of network usage fees on the Brazil cloud market, and* Analysys Mason (2020), *IP interconnection on the internet: a white paper.*

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

evidenced by recent research from the French regulator Arcep[53] and survey findings published by BEREC. Both studies found that transit (where no CDNs are involved) accounted for between a third and half of traffic. Importantly, third-party CDNs that act on behalf of CAPs are intermediaries and do not control or modify the content that these CAPs deliver to end users through CDNs. The relationship is first and foremost between these CAPs and their own customers, with CDNs and ISPs simply facilitating the flow of content from one to the other, with the highest quality and lowest cost possible.

53 Arcep (2024), *The State of the Internet in France*, Breakdown by origin of traffic to customers of the main ISPs in France (end of 2023).

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

In this section, we compare the dynamics at play in the telecoms and cloud sectors, and assess 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 need to first articulate the problem or market failure they are trying to solve. They should then 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 justified, proportionate, and consistent with the purpose of the telecoms regulatory framework.

EU law is based on a number of principles and fundamental rights, which are recognised by European case law and are relevant to regulation in the context of this paper. These include **proportionality**[54] and **purposive construction**,[55] as well as **equal treatment** before the law[56] and the **freedom to conduct a business**,[57] within the rules set by legislators:

- Proportionality requires that measures adopted by EU institutions must be appropriate and necessary to achieve the objectives pursued by the legislation, and they should not exceed what is necessary to achieve those objectives. When there is a choice between several appropriate measures, the least onerous option should be selected, and the disadvantages caused by the measures should not be disproportionate to the aims pursued.

- Purposive construction requires legal texts to be interpreted in a way that best achieves the objectives set out by the legislation, rather than adhering strictly to the literal meaning of the words. This means that to understand the scope of the telecoms regulatory framework, and in

54 Article 5(4) Treaty on European Union; Article 5, Protocol (No 2) Treaty on the Functioning of the European Union; affirmed by ECJ in series of cases including Federation Charbonnière (C8-55), Internationale Handelsgesellschaft (C11-70), Fedesa (C331-88), Swedish Match (C201-03) and Digital Rights Ireland (C293-12).

55 See: Telekom Austria v Mayer (Case C-491/04); Deutsche Telekom AG v European Commission (Case T-261/07); Vodafone Ltd v Secretary of State for Business, Enterprise and Regulatory Reform (Case C-58/08.

56 See: Arcelor Atlantique et Lorraine and Others v Premier ministre, Ministre de l'Écologie et du Développement durable, Ministre de l'Économie, des Finances et de l'Industrie (Case C-127/07); Finanzamt Köln-Altstadt v Roland Schumacker 2 (Case C-279/93), Spain v Commission (Case C-304/01).

57 See: Sky Österreich GmbH v Österreichischer Rundfunk (Case C-283/11), Alemo-Herron and Others v Parkwood Leisure Ltd (Case C-426/11), AGET Iraklis AE v Minister for Labour, Social Security and Social Solidarity (Case C-201/15).

particular the EECC, it is important to understand why measures were imposed – i.e. the problem they are seeking to address.

- Equal treatment mandates that comparable situations must not be treated differently and different situations must not be treated in the same way, unless such treatment is justified on the basis of an objective and reasonable criterion and is proportionate to the aim pursued in light of the fundamental objective.

- The freedom to conduct a business includes the right to engage in economic or commercial activity, freedom of contract, and free competition. These can be limited by law, as long as these limitations respect the essence of those rights and freedoms, and comply with the principle of proportionality. Such limitations must be necessary and genuinely meet objectives of general interest recognised by the EU or the need to protect the rights and freedoms of others.[58]

In order to expand the definition and application of the EECC to include any of these aspects of cloud, European policy makers would need to demonstrate that there are problems, including market failures, that are consistent with those the EECC was designed to address in the telecoms sector. They would also need to demonstrate that the application of the EECC would be justified and proportionate in addressing these problems. This section addresses these questions as follows:

- In Section 3.1, we summarise the history of sectoral regulation in European telecoms provided in Annex A, both from the perspective of policy objectives and the specific conditions in which the regulatory framework emerged and evolved over the last 40 years.

- In Section 3.2, we explore the distinct dynamics that characterise the cloud and telecoms sectors, highlighting the significant differences that exist between these sectors and how their requirements for regulation vary greatly, even if seeking to achieve similar policy objectives.

- In Section 3.3, we focus on specific areas where cloud and telecoms are intertwined. As discussed in Section 2.3, these include the private networks of cloud providers (including submarine cables), the connectivity required for cloud customers to access cloud services, and CDNs.

58 See *Charter of Fundamental Rights of the European Union*, Article 16 and Article 52(1).

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

Summary

The EU telecoms regulatory framework was put in place to facilitate evolution from state-owned national monopolies to an open, competitive sector. Extensive regulation was required to bring about this change. Some of these regulatory measures remain necessary and are still enforced to this day to address the specific challenges inherent to the telecoms sector.

Ex-ante regulatory intervention liberalised the telecoms sector (i.e. allowed new suppliers to offer telecoms services) by addressing specific barriers to entry and regulated actors with market power caused by persistent structural features of the telecoms sector. In addition, ex-ante regulation dealt with defined policy objectives and consumer protection issues. Over time, the regulatory framework transitioned from a patchwork of national approaches to a broadly harmonised set of European rules, implemented nationally through market assessment and enforcement by national regulators, overseen by the EC.

Continued areas of focus for telecoms regulation reflect this history. Market access is facilitated through the issuance of general authorisations, whilst the allocation of scarce resources, such as spectrum frequency licences and numbering, is handled in a more specific manner. Some structural issues are persistent, linked to network effects, economies of scale and scope, and enduring competitive bottlenecks. In particular, the strategic incentives of vertically integrated operators (which are prevalent in the sector) are addressed through interconnection and access requirements, including to infrastructure and wholesale services, and a dispute resolution mechanism. National regulatory authorities (NRAs) can only impose additional intrusive remedies if they have undertaken a detailed market analysis, approved by the EC.

Wider policy objectives addressed by the telecoms regulatory framework include access to emergency services and universal service, whilst consumer protection measures relate to end-user contracts and information.

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.

This is expanded further in Annex A.

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

Summary

The EECC framework is designed to address policy objectives within the specific dynamics of the telecoms sector. These dynamics include:

- The mature and stable nature of the telecoms sector, and the inherent inability of end users to self-supply in all but niche cases, created the condition for a durable monopoly despite liberalisation.
- Contestability[59] and competition issues relate in part to the late liberalisation of the sector (at a point when many people already had a phone line) and to persistently high barriers to entry, leading to significant and durable market power of former state-owned incumbents.
- Direct network effects associated with telephony, where the ability to reach another user was at the heart of the nature of the service, benefited large established network operators at the expense of new entrants.

The cloud services sector exhibits different dynamics, namely in its rapid growth which builds on businesses' existing demand for IT infrastructure and services, which 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. Direct network effects are also 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.

Various competition authorities in Europe (including the UK) have in recent years conducted assessments of the cloud sector, which have highlighted a number of potential issues relating to competition. Despite these issues, no regulatory interventions have been implemented to date. 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.

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, which are in the process of being implemented and whose effects must be assessed in due course.

Detailed references to the legal framework are provided in Annex B.

This section examines the rationale for the current EU telecoms regulatory framework from the perspective of the history of competition in telecoms, and the specific sector dynamics at play in the telecoms sector. We contrast those dynamics with those at play in the cloud sector to assess the relevance, justification and proportionality of applying the existing telecoms regulatory framework to cloud services. This is summarised in Figure 3.1 below.

We note that there are emerging competition concerns in the cloud sector, based on recent and ongoing market studies by EU and UK competition authorities, and highlight how these concerns differ from those addressed by telecoms regulation.

59 Contestability is defined as the ability and ease with which firms can enter or exit a market.

Figure 3.1: 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.[60] 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 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.	High levels of innovation to enhance user experience resulting 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.

60 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
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.

3.2.1 The regulation of telecoms recognises the maturity and stability of the telecoms sector, in sharp contrast with the current stage of development of the cloud sector, which is in rapid expansion

Cloud services are targeted at businesses, which are progressively migrating IT workloads from their own infrastructure to cloud platforms, resulting in the growth of the cloud sector

Unlike cloud services, which are primarily offered to businesses, telecoms services cater to both consumers and businesses of all sizes. These customers are often forced to enter into complex long-term contractual commitments to receive telecoms services. They also lack a credible means of using their own communications services, given the high costs and complexity of network deployment, and the importance of interconnection. A limited number of businesses with high connectivity requirements may be able to self-deploy networks, but typically rely on managed services provided by ISPs or enterprises connectivity providers.

As a result, the EECC contains detailed consumer protection rules for consumer and end-user contracts, and provisions on wholesale interconnection and access (including dispute resolution provisions) between telecoms operators to address long-standing concerns stemming from the factors described in Section 3.1.

In contrast, customers of cloud services are primarily businesses which, with the exception of recently emerging public-cloud native businesses, have historically self-supplied IT capabilities under a traditional 'on-premises' IT model as described in Section 2.2. Eurostat data for 2023 indicates that 54% of European businesses do not buy cloud services,[61] suggesting most businesses are continuing to self-supply required IT capabilities in full, whilst those businesses that do take at least some cloud services retain significant 'on-premises' capabilities as part of a hybrid architecture.[62]

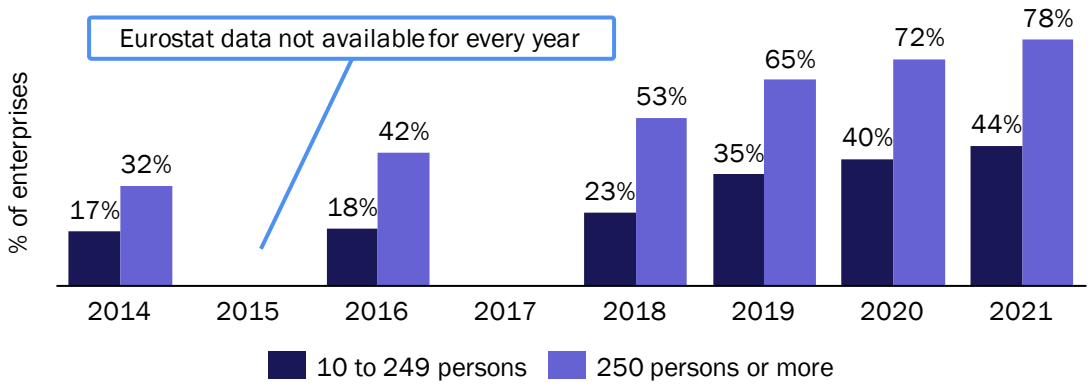
Adoption of cloud services by European businesses has continued to grow at a CAGR of 14% in the period 2018–2023, with the EU's digital decade targeting further take-up to reach 75% of businesses

61 Includes all activities except agriculture, forestry and fishing, mining and quarrying, and excludes the financial sector.
Eurostat, *Cloud computing services by NACE Rev.2 activity* (accessed July 2024).

62 A survey conducted by McKinsey, the results of which were published in April 2024, suggests that only 13% of cloud-using respondents had over 80% of workloads in the cloud, while 68% had fewer than 50%. See McKinsey & Company (2024), *The state of cloud computing in Europe*.

by 2030.[63] Take-up of cloud services in Europe is currently skewed towards larger enterprises,[64] in addition to 'digital native' start-ups and scale-ups, as reported by Eurostat (see Figure 3.2). Recent research released by the UK Competition and Market Authority (CMA) suggests that customer spend on public-cloud services in the UK is highly concentrated, with 50% of revenue being derived from 1% of customers.

Figure 3.2: Adoption of cloud services by size of business in the EU, noting that only a subset of cloud adopters' IT workloads are in a public cloud [Source: Eurostat, 2024][65]



This continued take-up of cloud services, combined with increasing use of cloud by existing customers (as reported by Ofcom that existing cloud customers continue to migrate more workloads to the cloud[66]), is resulting in continued revenue growth for the cloud sector. The Dutch Competition and Markets Authority (ACM) recently found revenue for European cloud services has grown at 20–30% per annum since 2017.[67] Ofcom reported a similar growth rate for the global spend on cloud services with an estimated 23% growth in 2023.[68]

By comparison, adoption of broadband and mobile services has grown at a CAGR of 2.5% and 0.5% respectively, over the period 2018–2023.[69] Revenue within the European telecoms business market has also been broadly stable in recent years, with a CAGR of –0.4% per annum in 2018–2022,[70] driven by existing high take-up levels and a reasonably standardised service offering. This variance

63 European Commission, DECISION (EU) 2022/2481 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 establishing the Digital Decade Policy Programme 2030.

64 Eurostat defines a large enterprise as having 250 or more employees.

65 Eurostat does not provide percentages for enterprises with fewer than 10 employees.

66 Ofcom (2023), Cloud services market study, p. 22.

67 Autoriteit Consumet & Markt (2022), *Market Study Cloud services*, p. 32.

68 Ofcom (2023), Cloud services market study, p. 21.

69 This is based on penetration rates, defined as the number of subscriptions per inhabitant. For telecoms, this is routinely above 100% to account for second homes, offices and secondary mobile handsets.

70 Total business retail revenue in Europe. For more information, see Analysys Mason's DataHub.

in growth rates highlights the differing levels of maturity between the telecoms sector, around which the EECC has been developed, and the emerging cloud sector.

The significant growth in the cloud sector, primarily driven by business IT spend, suggests significantly different market dynamics to those the EECC seeks to address in a telecoms sector characterised by very limited ability to self-supply and a diverse customer base consisting of both consumers and businesses of all sizes.

The structure of the telecoms and cloud sectors reflects their distinct histories, varying degrees of vertical integration and differing levels of maturity

Supply in the telecoms sector remains relatively concentrated, as discussed in Section A.2, as a result of a history of state-owned monopoly. In fixed telecoms, competition was introduced in a sector where a large majority of potential customers were already served by the incumbent. As a result, any player entering the market after liberalisation had to contend not only with intrinsic barriers to entry, but also with a mature market with a strong incumbent.

The EECC recognises the enduring impact of this history, by maintaining ex-ante regulation for a small number of relevant markets (primarily related to interconnection and access), and the option for NRAs to investigate other markets that pass a three-criteria test[71] and where an operator may have significant market power (SMP).

In contrast, cloud services started as inherently competitive services. Since the launch of AWS in 2006, cloud providers have worked to expand their customer base by convincing businesses to move IT workloads from their own IT infrastructure to the cloud.

Furthermore, as discussed in Section A.2, the telecoms industry has historically been, and to a significant extent remains, vertically integrated with passive and active infrastructure owners also providing services directly to end users. This, as discussed in Annex A, has created an incentive for operators to refuse or obfuscate interconnection with new entrants to limit retail competition. Recent trends towards 'delayering' of infrastructure, networks and services are still at an early stage, and most infrastructure providers have 'anchor tenants', well-established operators that are dependent on this infrastructure and are major customers to the infrastructure provider, with broadly aligned strategic incentives.[72]

The EECC recognises the structural prevalence of vertical integration, so that ex-ante regulation can apply to operators with SMP in specific markets, to try and prevent these factors from negatively affecting competition. Since 2020, the only two markets that the EC specifically directs NRAs to review are the markets for "wholesale local access provided at a fixed location" and for "wholesale dedicated capacity".

71 See Annex A.3, footnote 184.

72 BEREC (2023), *Study on the evolution of the competition dynamics of tower and access infrastructure companies not directly providing retail services.*

Some vertical integration does exist within the cloud sector, with some major cloud providers supplying infrastructure as a service (IaaS), platform as a service (PaaS) and software-as-a-service (SaaS) solutions, and recent studies from European competition authorities identifying software licensing practices as potential concerns (discussed further in Section 3.2.3). However, any concerns that may exist are fundamentally different to those created by vertical integration in the telecoms sector in two main ways:

- First, the major public-cloud providers host a large number of ISVs, which offer a wide variety of services (as shown previously in Figure 2.3). Cloud providers provide inputs to ISVs, and a route to market through marketplaces; they also compete in some areas, whilst larger ISVs have the option to buy lower-level inputs from cloud providers to replicate some of their software building blocks.[73]

- Second, as discussed in Section 2.2.3, a cloud user can realistically directly access any part of the value chain, giving it the ability to self-supply certain (or all) elements of its IT stack and hence avoiding the requirement to take all services from a single vertically integrated provider. Cloud users can and do move workloads out of the cloud entirely, for example once they reach a certain scale or if this is more economical given their requirements.[74]

As discussed previously, this option does not really exist in telecoms, except in very niche scenarios in which companies have the scale, expertise and incentive to deploy their own private networks. For mobile communications, technical constraints linked to the licensing and co-ordination of spectrum bands have made this largely impossible so far outside of limited 'campus' style deployment.

As a result of these key differences in levels of vertical integration, self-supply and associated incentives between telecoms and cloud sectors, the mechanisms imposed by the EECC do not appear appropriate to address any concerns that may arise in the cloud sector.

Cloud services require substantial capital investment on a global scale, in contrast with telecoms' localised infrastructure needs, and are also much more R&D intensive than telecoms

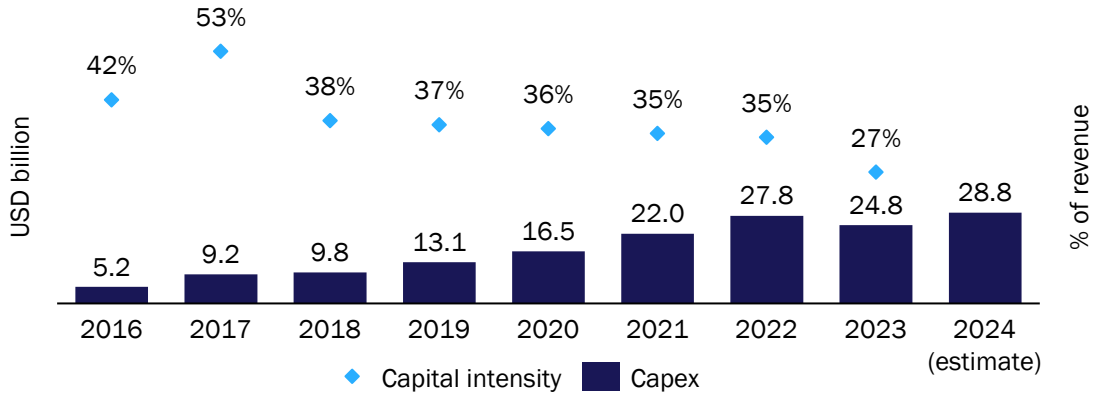
Cloud and telecoms are both capital-intensive sectors. As outlined in Section A.2, European telecoms operators have sustained a capex intensity of between 15% and 20% since 2015, with an average of 18% across the period. By comparison, capex intensity for AWS, as shown in Figure 3.3, averages 35% in the period since 2016, driven by strong revenue growth, resulting in a signifcant increase in overall investments.

---

73 For example, certain Oracle PaaS products can be run in non-Oracle cloud environments, such as hyperscaler clouds.
Autorité de la concurrence (2023), *Opinion 23-A-08 of 29 June 2023 on competition in the cloud sector*, p. 133.

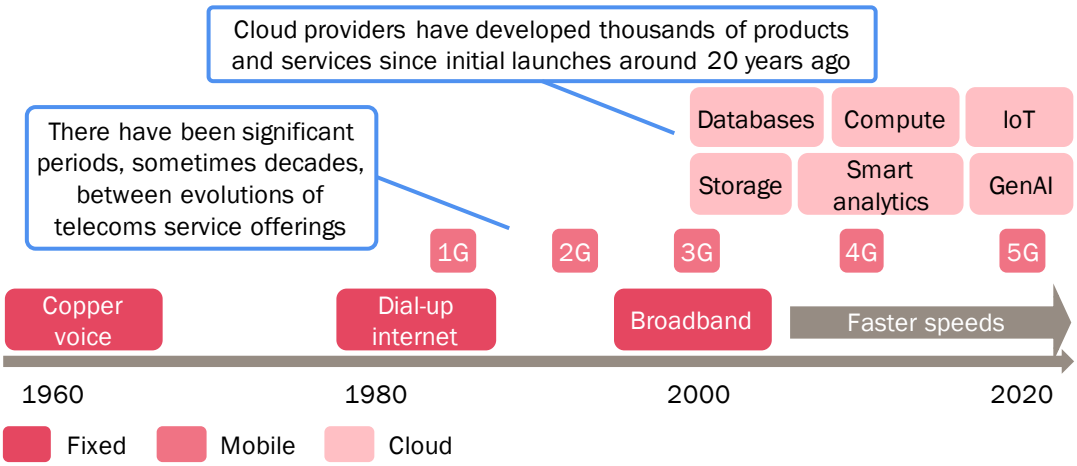
74 BBC (2024), *Are rainy days ahead for cloud computing?*

Figure 3.3: Evolution of AWS's capex intensity [Source: AWS annual reports, Analysys Mason, 2024][75]



The telecoms sector exhibits long investment cycles, driven by the importance of standardisation (including through international organisations such as ITU) and a high degree of technological maturity, which make incremental innovation long and complex. Significant innovations, such as the roll-out of 5G networks or fibre, involve long-term projects requiring extensive standardisation, testing and deployment, on both the network and end-user device side. For example, the full implementation of 5G across Europe is projected to span several years, with roll-out only targeted to be finalised by around 2030,[76] and the current cycle of national scale fixed infrastructure roll-out with fibre, was preceded by the roll-out of copper networks, some 60 years ago, as illustrated in Figure 3.4.

Figure 3.4: Major infrastructure roll-out in fixed, mobile and cloud [Analysys Mason, 2024]

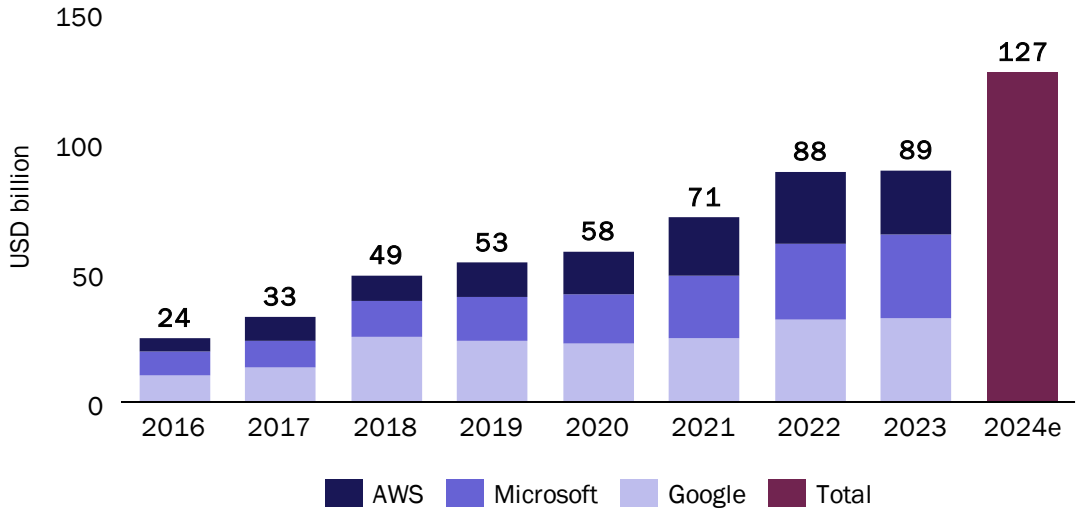


75 In this figure, we use net addition to property and equipment as a conservative proxy for capex. Amazon reported total capex of USD58 billion in 2022 and USD48 billion in 2023, driven primarily by AWS, which suggests actual capex intensity for AWS is higher than illustrated in the chart. AWS presented as example for cloud operators as Google and Microsoft do not provide financial breakdowns for cloud operations. 2024 estimates based on Amazon capex guidance suggest an increase of 16% in 2024 at group level.

76 European Commission, *Shaping Europe's digital future: 5G.*

In contrast, cloud providers must invest to increase the capacity of their services to meet growing customer demand for not only more of their existing services, but also for innovative and new services: servers and other active equipment typically constitute the largest expense.[77] As a result, capex spend from the main public-cloud providers has continued to increase, as shown in Figure 3.5, in recent years as demand for cloud services has continued to grow.

Figure 3.5: Evolution of capex spend by hyperscale cloud providers; for Google and Microsoft this is for the whole company as cloud capex is not reported separately [Source: Hyperscaler annual reports, Analysys Mason, 2024][78]



The expected economic lifetime for servers is around five years,[79] whereas telecoms operators typically depreciate their network investments over eight to ten years for active equipment, and much longer periods for passive equipment. Short investment cycle fosters a dynamic environment where providers can rapidly deploy new technologies and services. For example, the recent increase in demand for generative AI resources has been referenced as a key driver for increased capex investments in the earnings calls for Q1 2024 for AWS, Microsoft and Google:

> "We expect the combination of AWS's reaccelerating growth and high demand for gen AI to meaningfully increase year-over-year capital expenditure in 2024, [which means we] have to procure new data centres, power, and hardware." – *Andrew Jassy, CEO Amazon*[80]
>
> "We expect capital expenditures to increase [...] driven by investments in our cloud and AI infrastructure." – *Amy Hood, CFO Microsoft*[81]

77 DGTL Infra (2024), *Cloud and Hyperscale Capital Expenditures (CapEx) in 2024.*

78 Estimates for 2024 based on Q1 reporting and companies' capex guidance for the year.

79 Data Center Frontier (2022), *Sturdier Servers: Cloud Platforms Say Servers Living Longer, Saving Billions.*

80 Amazon (2024), *Amazon.com, Inc.: Q1 2024 Earnings Call.*

81 Microsoft (2024), *Microsoft FY24 First Quarter Earning Conference Call.*

> "We are committed to making the investments required to keep us at the leading edge in technical infrastructure. You can see that from the increases in our capital expenditures. This will fuel growth in Cloud, help us push the frontiers of AI models, and enable innovation across our services, especially in Search." – *Sundar Pichai, CEO Alphabet and Google*[82]

The result of such rapid investment cycles is continued innovation as each cloud provider, leveraging its R&D function as discussed below, looks to increase its efficiencies and improve its customer offering upon equipment refresh. This continued innovation towards differentiated products shows a considerable difference compared to the telecoms industry's long-term investments in standardised services. This translates into very different spend on R&D between key players in the telecoms and cloud sectors, as illustrated by data from the EU's industrial R&D scorecard in Figure 3.6 below. Whilst the R&D intensity of network and other equipment vendors is similar to that of cloud providers, operators spend much less on R&D as a share of revenue.

Figure 3.6: Overview of R&D spend by key players in the cloud and telecoms sectors [Source: EU Industrial R&D Investment Scoreboard, 2023]

Sector	Company	R&D intensity	R&D spend (EUR billion)
Software and computer services (327 companies)	Alphabet	14%	37
	Meta	29%	32
	Microsoft	13%	25
	Other	13%	147
Fixed and mobile operators (29 companies)	Various	3%	18
Technology hardware and equipment (216 companies)	Huawei	18%	21
	Nokia	17%	5
	Ericsson	24%	4
	Others	9%	165

The characteristics of the cloud and telecoms sectors also result in very different barriers to entry and expansion, which we discuss below.

3.2.2 Telecoms regulation addresses specific barriers to entry, competitive dynamics and network effects, which are very different from those present in the cloud sector

In this section, we examine how the telecoms regulatory framework addresses contestability and market entry, competition between suppliers, and the specific question of network effects in the telecoms sector. In summary, we draw the following distinctions between the cloud and telecoms sectors:

82 Alphabet (2024), *2024 Q1 Earnings Call.*

Contestability in the telecoms sector is conditioned in part by barriers to entry including licensing, availability of spectrum, and the nature of economies of scale and up-front investments:

- Entering a mature market (like the telecoms sector) where everyone has a fixed line is different from entering a fast-growing sector (like the cloud sector).
- Information society services, including cloud services, other than telecoms have been deliberately excluded from any licensing or authorisation regime.
- Cloud and telecoms exhibit very different infrastructure-related barriers to entry.
- Service-based competition based on wholesale access to telecoms networks offered an alternative route to a 'ladder of investment' in telecoms, which market forces appear to be offering already in the cloud.

Competition in telecoms is characterised by a high degree of standardisation and commoditisation at all levels, with barriers to switching mirroring barriers to entry throughout the value chain:

- Standards and interoperability play a different role in facilitating competition and switching.
- Using multiple providers at the same time is physically challenging in telecoms because of infrastructure limitations and largely commoditised products. This creates an 'access monopoly' for a given customer at a given point in time, which does not exist in the cloud sector.

Direct network effects are not a feature of the cloud sector and are becoming progressively less important in telecoms, as applications that exhibit network effects move away from the network.

Contestability in the telecoms sector is conditioned in part by barriers to entry including licensing, availability of spectrum, and the nature of economies of scale and up-front investments

- *Entering a mature market where everyone has a fixed line is different from entering a fast-growing sector*

The differences in maturity between telecoms and cloud, including the high penetration of fixed telephone lines at the point when the telecoms sector was liberalised, are indicative of very different contestability dynamics: a new entrant coming into telecoms has to acquire customers that are already served by incumbents, in a relatively slow-growing (or in some cases declining) overall revenue pool, whereas new cloud providers can compete "for the market"[83] and aim at gaining share of a fast growing revenue pool. Since at least 1999, the EC has recognised the need for regulation to enable new entry and competition through interconnection and access, and to address consumer issues including the ability to call emergency services have number portability and minimum

83 See Autorité de la concurrence (2023), *Opinion 23-A-08 of 29 June 2023 on competition in the cloud sector*, p. 186.

information about contracts and tariffs.[84] As such, telecoms regulation has been constructed from the start with the need to ensure new entry is efficient and facilitated in ways that could enhance consumer welfare, despite the maturity of the sector.

- *Information society services other than telecoms have been deliberately excluded from any licensing or authorisation regime*

As part of the liberalisation process of the telecoms sector (see Annex A), an important step was the removal of '*special and exclusive rights*' to supply telecoms services which, coupled with the introduction of general authorisations, enabled market liberalisation and entry by new providers into a sector dominated by state-owned monopolies before 1998.

This removed discretionary barriers that NRAs and governments could impose to limit entry into their national telecoms sector. The 'general authorisation' regime has made it much easier for new telecoms providers to enter new Member States: market entry is now only conditioned on compliance with national conditions of general authorisation. In addition, access to scarce, nationally managed resources including telephone numbers and radio spectrum are subject to specific licensing requirements.

In contrast, as other digital services developed, no historical 'special and exclusive rights' existed and there were no licensing requirements (i.e. there was an absence of regulatory barriers to entry, either at EU level or in individual Member States).

In fact, applicable regulation sought to ensure that no regulatory barriers to entry could be imposed: e-Commerce Directive (Art. 4 (1)) provides that:

> "Member States shall ensure that the taking up and pursuit of the activity of an information society service provider may not be made subject to prior authorisation or any other requirement having equivalent effect", except in the context of telecommunications services specifically.[85]

Further details on information society services are provided in Annex B.4.

- *Cloud and telecoms exhibit very different infrastructure-related barriers to entry*

As set out in Section A.1, barriers to entry in telecoms are heavily conditioned by the complexity and high up-front capital cost of establishing a telecoms network. Building fixed or mobile networks aimed at providing electronic communication services to the public involve large-scale investments in infrastructure, with long payback periods.

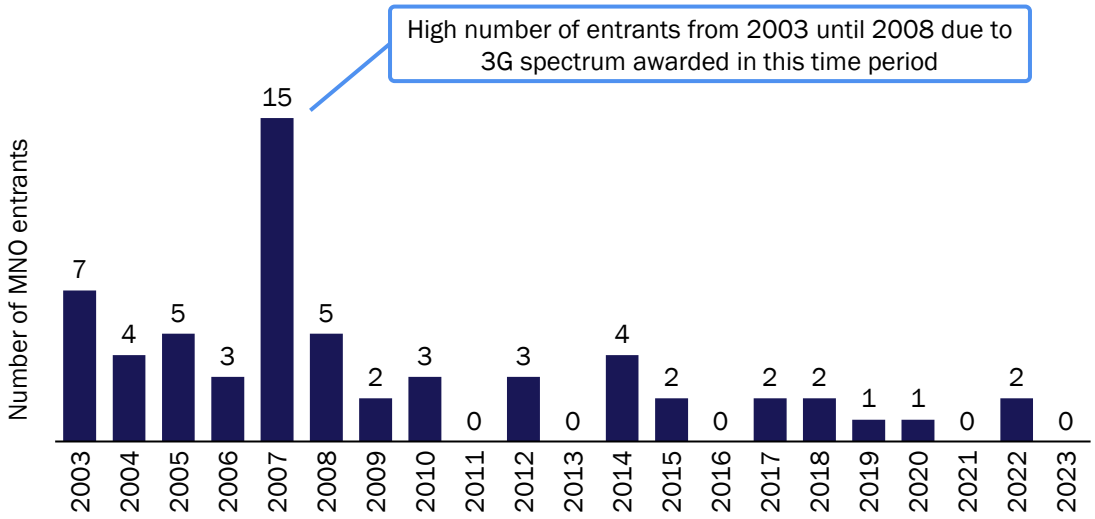
---

84 European Commission (1999), *Towards a new framework for Electronic Communications infrastructure and associated services: The 1999 Communications Review.*

85 European Commission (2000), *Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce').*

As a result, as shown in Figure 3.7, there have been relatively few infrastructure-based new mobile entrants in the EU over the last 20 years.[86] The analysis shows that, although there were a relatively higher number of entrants between 2003 to 2008 (at which time 3G spectrum auction rules often facilitated a new entrant), there has been a reduction since 2008 and the overall volume across the whole period is low.

Figure 3.7: New entrants in the European mobile telecoms sector in the past 20 years [Source: GSMA, Analysys Mason, 2024



Beyond access to spectrum in the mobile sector, barriers also remain high for fixed telecoms operators, particularly for 'last-mile' connectivity to end users. Digging up roads to lay cables is expensive, often impractical, and very time consuming. An essential characteristic of telecoms networks is that they must be deployed where customers are, and in turn customers can only access networks that are deployed to their locations.

The EECC includes several provisions aimed at facilitating market entry, covering access to spectrum, and both active and passive infrastructure. Relevant articles and their purposes are provided in Annex B.1.

By comparison, new cloud services can be launched with relatively limited initial investment, by leasing space in co-location data centres and using standardised, open-source tools and platforms. As an example, this is visible in the rapid expansion of AI-focused cloud service providers such as CoreWeave. Location can be important in the context of performance and compliance with data sovereignty rules, albeit to a subset of cloud users only.[87] In addition, these requirements do not impose that data centres must be deployed in specific locations within an individual country or

86 Mobile virtual network operators (MVNOs) are excluded for the purposes of this example as they do not face the same barriers to the deployment of infrastructure.

87 Autorité de la Concurrence (2023), *Opinion 23-A-08 of 29 June 2023 on competition in the cloud sector*, p. 74.

region, and in fact even very large cloud providers tend to operate few data-centre locations in each country.

- *Service-based competition offered an alternative route to a 'ladder of investment' in telecoms, which market forces appear to be offering already in the cloud*

Barriers to entry in the infrastructure level can be circumvented if entry is possible at the service level. This entails the use of an infrastructure operator's network on a wholesale basis, to sell services to the end user at the retail level. Infrastructure owners that also offer retail services (including former state-owned incumbent operator) often have limited incentive to provide access to the network, or to provide access at a price that allows new entrants to compete with them on retail markets.

Regulation of the telecoms industry dealt with this challenge through imposing interconnection (later extended to access) obligations. Whilst ex-ante regulation has been effective in imposing basic interconnection and access obligations in defined markets, it has been much less effective at dealing with abusive behaviour by vertically-integrated dominant telecoms operators (often across adjacent markets) and issues such as 'failure to supply services' (not within the scope of the regulated interconnection obligation) and pricing behaviours such as 'margin squeeze' were instead addressed by general competition law in a series of cases in the telecoms sector.[88]

By comparison, new entrants in the cloud sector have pursued different routes to market (as discussed in Section 2.2.2).

Initial investment restrictions to enter the cloud sector can also be further reduced at the PaaS level through the 'virtual' cloud provider model in which a cloud provider rents compute power within a larger cloud providers network on which to deploy and sell its own platform. This is comparable to a wholesale infrastructure access model in the mobile telecoms market and reduces the infrastructure required to virtually nil. However, it is worth noting that the use of this model in the cloud industry, particularly in the development of a platform, allows for greater service differentiation, and therefore ability to compete, than in the telecoms industry where services are relatively standardised.

Agreements of this nature already exist in the cloud sector with PaaS providers offering services that are based on the infrastructure of different cloud providers. For example, Ofcom found that IBM is making its cloud infrastructure services available in any data centre, including AWS and Azure.[89]

The differences in barriers to entry and persistent structural features between the telecoms and public-cloud sectors clearly demonstrate that sector-specific interconnection (later extended to

88 Deutsche Telekom AG v European Commission, Case C-280/08, France Télécom SA v Commission of the European Communities, Case T-340/03, Konkurrensverket v TeliaSonera Sverige AB, Case C-52/09, Telefónica SA and Telefónica de España SAU v European Commission, Case C-295/12, Slovak Telekom, a.s. v European Commission, Case T-851/14.

89 Ofcom (2023), *Cloud services market study*, p. 114.

access) regulation, which has been deployed to address these issues in the telecoms sector, is neither necessary nor proportionate for the public-cloud sector (see Annex B.3).

Competition in telecoms is characterised by a high degree of standardisation and commoditisation at all levels, with barriers to switching mirroring barriers to entry throughout the value chain

- *Standards and interoperability play a different role in facilitating competition and switching*

The telecoms sector is built around global standards, discussed and agreed in international forums including the ITU, enabling a high degree of interoperability and compatibility. This translates into highly standardised retail services too: the set of functionalities that mobile standards enabled until the most recent versions of 5G were primarily centred around messaging and calls, and internet access services are sold on the basis of coverage, speed and volumes of included data.[90] Most mobile devices are designed to work with any provider, and fixed broadband equipment has evolved so that much of it is self-supplied by end users (Wi-Fi and local-area network equipment), with only the entry point into the customer's premises being controlled by an operator's gateway equipment.[91]

In the cloud sector, standards also play an important role in the fundamental building blocks of compute, storage and networking, but less so in the context of cloud services themselves. Cloud users can access cloud services over the public internet from any connected devices, and use standards-based resources from 'bare metal' infrastructure to software building blocks. Unlike in telecoms, however, there are hundreds of individual services available on cloud platforms, offering a high degree of differentiation and customisation. Some of these building blocks are specific to some cloud platforms (e.g. Amazon RedShift), and as discussed in Section 3.2.3, this gives rise to specific concerns around interoperability and switching costs, which do not exist in telecoms.

There is a link between innovation and standardisation, which would be very hard for regulators to mandate or direct. Telecommunications standards are highly interoperable, enabling economies of scale across thousands of networks operating independently across the world. This requires a high degree of standardisation, achieved through long and complex international processes at organisations such as ITU and 3GPP. Conversely, cloud services benefit from global economies of scale within individual platforms, without the need for these international standardisation processes, which leads to faster innovation.

- *Using multiple providers at the same time is physically challenging in telecoms because of infrastructure limitations and largely commoditised products, unlike in the cloud sector*

Further challenging the competitive landscape, both businesses and consumers typically do not use multiple providers at once ('multi-home') and rely on a single telecoms provider for each major

90 Primary research surveys undertaken by Analysys Mason indicate price satisfaction and coverage satisfaction are two of the primary drivers of churn in developed countries.
Analysys Mason (2023), *Mobile customer satisfaction and experience: consumer survey*.

91 Broadbandbuyer.com, *GPON ONT (Optical Network Terminal)*.

service (e.g. last-mile fixed connectivity, mobile services, machine-to-machine communication). [92] This dynamic can partially be attributed to the location-centric nature of telecoms networks, as a consumer or business may have limited or no choice in alternative (passive infrastructure) providers for their location. In the context of fixed networks, the final drop into the customer's premises also cannot typically be used by multiple providers concurrently. Historically, multi-homing was further limited by the importance of telephone numbers, which are assigned to an individual provider, although this is changing in mobile in particular thanks to the popularity of over-the-top communications services.

Customer switching between telecoms providers does occur, although often this is only at the retail level, and not as frequently as might be in the customer's interests, suggesting some non-trivial barriers to switching exist.[93] For fixed telecoms services at the wholesale or passive infrastructure, level, while fixed infrastructure overbuild exists for commercially attractive areas, many rural areas rely on state subsidies for build-out, meaning that the availability of alternative providers is often limited, or non-existent. This means, even if a customer can switch at a retail level, the available service, as determined by the network infrastructure, may not be improved.

The EECC includes several provisions to facilitate switching between telecoms operators. Some of these provisions are specifically focused on consumers, understood as individuals and small businesses. Large enterprises, which form the bulk of the demand for cloud services, are not directly covered by many of these provisions. These provisions are highlighted in Annex B.2.

The modular and standardised nature of cloud services allows enterprises to use a range of hybrid and multi-cloud approaches based on their needs at a given time. The use of multi-cloud solutions varies across geographies, industries and organisations at varying stages of digital transformation. Technical and commercial barriers to multi-cloud adoption are being reviewed by competition authorities, as discussed briefly in Section 3.2.3 below.

Despite potential barriers, cloud users are consistent in their intention to increase use of multi-cloud in the future.[94] Beyond increasing digital transformation, one of the key drivers towards multi-cloud is seen as finding the right cloud platform for the application,[95] which suggests organisations may increasingly look to smaller niche providers to leverage their specialised capabilities. For the many enterprises with already well-established cloud capabilities, their use of different cloud platforms remains dynamic. A significant proportion of these enterprises have reported moving workloads

92 I.e. an individual or household may subscribe to multiple telecoms services (e.g. fixed broadband, mobile, pay TV) and these services may come from different providers. However, individual subscribers do not generally have multiple fixed broadband connections and, in developed markets (without extensive mobile coverage issues), relatively rarely subscribe to multiple mobile services.

93 Ofcom Switching Tracker suggests that consumers' key challenges to switching are timing the switch to maintain service whilst also not paying both providers simultaneously, and time/effort required to go through the switching process. See Ofcom (2022), *Core Switching Tracker Study 2022, July-August 2022*.

94 See for example: S&P Global Market Intelligence (2023), *Multicloud in the Mainstream: Making IT Work 'As Advertised'*, p. 1, which shows that 98% of enterprises surveyed have at least two cloud providers; Cloudtech (2024), *64% of organisations see their use of multi-cloud increasing in the next two years,* Nutanix (2023), *6th Annual Nutanix Enterprise Cloud Index.*

95 Cloudtech (2024), *64% of organisations see their use of multi-cloud increasing in the next two years.*

between cloud providers in the last two years,[96] with interoperability and data portability further supported by the EU Data Act,[97] which aims to reduce vendor lock-in and foster a competitive environment.

Direct network effects are not a feature of the cloud sector and are becoming progressively less important in telecoms, as applications that exhibit network effects move away from the network

Concentration in the telecoms sector has historically been influenced by network effects, where the value of services increases with the number of users, benefitting larger networks. In traditional telephony, network effects are evident in call termination rates, where receiving networks charge fees for terminating calls from other networks. Larger networks achieve economies of scale, leading to lower costs and competitive advantages over smaller operators, but also strategic incentives (arising from vertical integration) to obstruct interconnection, creating barriers for new entrants, as discussed in Section 3.1.

In the context of interpersonal communication services, network effects are shifting from the network to the application layer as an effect of digitalisation.[98] This shift is recognised in the EECC, which addresses both number-dependent and independent interpersonal communication services. However, for traditional telephony, these effects remain network-attached, justifying the continued inclusion of specific regulatory provisions.

The EECC includes several provisions aimed at ensuring fair and reasonable interconnection and access, as well as effective dispute resolution mechanisms. It also recognises the emergence and popularity of interpersonal communications services, both dependent and independent of telephone numbers. The key articles and their purposes, as articulated in the recitals, are provided in Annex B.3.

While the public-cloud business model benefits from aggregating demand from many customers to enable synergies and economies of scale, cloud services are not reliant on direct network effects.

Each customer's use of a cloud service is independent, relying on the public internet or private connections for any necessary linkages. This independence means the value of the cloud service for one user is not directly affected by the number of other users on the same platform. This structural characteristic allows cloud providers to start small and focus on optimising their services for individual performance and reliability rather than network scale.

Competition authorities that have conducted cloud 'market studies' have pointed out some indirect network effects, associated with ISV marketplaces. The more customers a cloud platform has, the

96 Enterprise Strategy Group eBook (2023), *Multicloud Application Deployment & Delivery Decision Making*.

97 European Union, *Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act)*, Section VIII Interoperability (2023, 2023/2854).

98 The internet separates the networks from the applications they support, enabling network effects to develop at the application layer regardless of the underlying networks used for access.

more attractive it is to ISVs. Likewise, if multi-cloud is complex or expensive, cloud users may prefer cloud providers with a greater choice of ISVs.

3.2.3 Emerging competition concerns in the cloud sector are very different from those in telecoms, further highlighting the lack of relevance of including cloud services under EU telecoms regulation

Recent studies by competition authorities in several European countries (including the UK) have highlighted concerns related to competition in the cloud sector

The rapid growth and increasing importance of cloud services for many businesses have raised interest relating to the competitive landscape in the sector among regulators worldwide. Regulators in Europe, including the Autorité de la Concurrence in France, ACM in the Netherlands, as well as Ofcom and CMA in the UK, have initiated reviews of the cloud sector.

These studies highlighted specific concerns about the way competition works in the cloud sector, but so far have not led to any decision to intervene in the cloud sector. Without prejudging the outcome of these processes, it is worth noting the issues that have been raised, and contrast them with those that the telecoms regulatory framework is designed to address.

Vendor lock-in is a concern raised in all studies. Lock-in occurs when customers face substantial barriers that prevent them from switching between cloud providers, creating a dependency on a single provider. These barriers can be technical or commercial, making it challenging for customers to migrate their data and applications to other providers without incurring significant costs or operational disruptions.

Technical barriers to switching

Technical barriers to switching include the complexities involved in transferring data and applications between different cloud environments. Each cloud provider often uses proprietary technologies, APIs and data formats, which can make interoperability difficult. As a result, customers may need to undertake extensive re-engineering of their systems to adapt to a new provider's infrastructure. For instance, applications developed on one provider's platform may require significant modifications to function on another provider's platform, leading to increased time and cost. Technical barriers contributing to vendor lock-in are highlighted by ACM,[99] Autorité de la Concurrence,[100] CMA[101] and Ofcom.[102]

99 Autoriteit Consumet & Markt (2022), *Market Study Cloud services*, p. 56.

100 Autorité de la Concurrence (2023), *Opinion 23-A-08 of 29 June 2023 on competition in the cloud sector*, p. 128.

101 Competition and Market Authority (2024), *Cloud Services Market Investigation Qualitative Customer Research*, p. 44.

102 Ofcom (2023), *Cloud services market study OFCOM market study*, p. 214.

Commercial barriers to switching

Commercial barriers to switching are highlighted in each of the studies[103] and concentrate on:

- Egress fees: these are charges imposed by cloud providers when customers move data out of their systems. They are often priced per gigabyte transferred and create a financial disincentive for customers to use multiple cloud platforms where large volumes of data would need to go from one cloud to another.
- Cloud credits: some providers offer credits of USD100 000 or more[104] as incentives for new customers or as part of enterprise agreements. These credits typically have expiration dates and are non-transferable. This creates a 'use it or lose it' scenario, encouraging customers to continue using a particular provider even if they are considering switching.
- Committed spend discounts: these are volume-based discounts offered in exchange for long-term commitments or minimum spending levels. While they can provide cost savings, they also create financial penalties for reducing usage or switching providers before the commitment period ends.

Software licensing practices

Software licensing practices are another common concern for regulators highlighted in market studies. These practices are seen as affecting competition, interoperability, and user freedom to choose or switch providers.[105]

Cloud service providers may use self-preferential licensing in bundling their cloud infrastructure services with their own software products. This bundling can discourage customers from using third-party software or switching to other cloud providers due to integrated features that work best within their

103 Autoriteit Consumet & Markt (2022), *Market Study Cloud services,* p. 57,
Autorité de la Concurrence (2023), *Opinion 23-A-08 of 29 June 2023 on competition in the cloud sector*, p. 146,
Competition and Market Authority (2024), *Cloud Services Market Investigation Qualitative Customer Research,* p. 66,
Ofcom (2023), *Cloud services market study OFCOM market study*, p. 214,
Japan Fair Trade Commission (2022), *Report on Trade Practices in Cloud Services Sector, p. 79,*
Federal Trade Commission (2023), *Solicitation for Public Comments on the Business Practices of Cloud Computing Providers.*

104 Autoriteit Consumet & Markt (2022), *Market Study Cloud services*, p. 45.

105 Autoriteit Consumet & Markt (2022), *Market Study Cloud services,* p. 61,
Autorité de la Concurrence (2023), *Opinion 23-A-08 of 29 June 2023 on competition in the cloud sector*, p. 143,
Competition and Market Authority (2024), *Cloud Services Market Investigation Qualitative Customer Research,* p. 83,
Japan Fair Trade Commission (2022), *Report on Trade Practices in Cloud Services Sector, p. 81,*
Federal Trade Commission (2023), *Solicitation for Public Comments on the Business Practices of Cloud Computing Providers.*

> ecosystem. Such practices can limit the ability of smaller software vendors to compete on a 'level playing field', as they are unable to offer the same integrated benefit.

The complexity of these competition authorities' market studies, including the ongoing scope and depth of the UK CMA's investigation,[106] demonstrates the specific nature of the dynamics at play in the cloud sector, and the need for a similarly specific approach to any regulatory intervention. We note that the combination of concerns from competition authorities and statutory provisions in the Data Act already appears to have had an impact on commercial barriers to switching, as Microsoft, AWS and Google have all reduced egress fees to zero for customers migrating out of their platforms. Software licensing practices remain a contentious area, which has not been addressed by regulation but has been subject to litigations and out-of-court negotiations.[107]

The telecoms regulatory framework is not intended to address these issues and would not be able to do so in a proportionate and effective manner

Possible competition issues highlighted in the various competition authorities' cloud studies reflect concerns that the largest cloud providers may be able to maintain or increase their share of cloud demand even as the sector develops further. However, the potential issues raised by competition authority reviews to date do not have parallels in the telecoms sector and as such use of the EECC framework would not be appropriate to address any concerns.

Technical barriers to switching in the cloud sector arise from the rapid pace of innovation in cloud, with all cloud providers investing in significant R&D activities to improve end-user experiences, as discussed in Section 3.2.1. This necessarily results in reaching solutions to customer challenges that are not immediately replicable by other cloud providers. By comparison, as discussed in Section 3.2.1, the telecoms sector is in a more mature state. This is reflected in the form of relatively standardised product offering for individual services (e.g. broadband connectivity, voice services) that are based on stable international standards developed over long time periods.[108] The EECC's guidance on standardisation is designed to support interoperability between standardised telecoms products and so its application to highly complex, diverse and rapidly developing cloud services would not be appropriate.

Variations of the commercial barriers to switching, as identified by the various competition authorities, are also present to some extent in the telecoms industry. The application of SMP regulation pursuant to the EECC to manage such barriers can only be undertaken under the EECC if a market satisfied the three-criteria test and an operator is found to have SMP.[109]

---

106 The investigation is expected to take 19 months with CMA having prepared and published over 650 pages of working pages and primary research to date (as of July 2024).

107 CISPE (2024), *CISPE and Microsoft Agree Settlement in Fair Software Licensing Case.*

108 Development of the 5G standard began in 2019, four years before its widespread deployment, European 5G Observatory.

109 Article 67(1) EECC, see Annex A.3 footnote 184184.

As such, it is not clear whether the cloud sector would satisfy these tests in order for any intervention under the EECC. The cloud sector exhibits lower barriers to entry than the telecoms sector, and the structure of the sector has never been a monopoly and there is vigorous competition between large providers.[110] In addition, the cloud sector is already subject to European competition law, and to various regulations including the Data Act, as discussed further later in this section. As such, it would be necessary to identify specific areas of defined barriers to entry that are not already addressed by these laws for the EECC's SMP remedies to be applied.

An additional complexity relates to the geographical scope of regulation. Basic telecoms services are inherently 'local' – they require a last-mile local connection to a customer (which could be fixed or wireless) which is always clearly within the jurisdiction of a particular Member State. The EECC reflects that reality, with each Member State implementing the EECC into local law then taking responsibility for regulating telecoms operators within its jurisdiction. In contrast, cloud services are inherently 'location independent' – they can be accessed by a customer anywhere in the world provided that the customer has an internet connection. The existing European approach to cloud regulation reflects this: Article 3 of the E-Commerce Directive sets out the country-of-origin principle, which is a key measure to enable a single market in information society services, Article 65 of General Data Protection Regulation (GDPR) establishes the competence of a lead supervisory authority to act a single point of contact for EU data protection, whilst both the Digital Services Act and Digital Markets Act recognise the role of the EC in addressing EU-wide issues. Any extension of the existing EECC to cloud services would create jurisdictional uncertainty and could adversely affect the single market[111] for cloud services.

Finally, we note that telecoms equipment, like cloud services used by telecoms operators, is outside the scope of the EECC. This being said, they are constrained by regulatory obligation that apply to telecoms operators but 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 the services they 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.[112]

Competition authorities recognise the range of regulatory tools available at EU level that may help address some of their concerns

The cloud sector is subject to a range of regulations in the European Union, which are being implemented and enforced in ways that seek to address some of these specific issues (e.g. the Data Act includes provisions that affect egress fees). This is in addition to general regulation, including competition law and consumer protection law (in cases where it applies).

110 Ofcom (2023), *Cloud services market study*, p. 34.

111 Depending on the circumstances, this may be incompatible with EU law: see Case C-344/04, IATA and ELFAA.

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

These laws and regulations are designed to ensure data protection, cyber security, fair competition and data portability. Key regulations include GDPR, the Digital Markets Act the Digital Services Act, the Data Governance Act, the Data Act, and the Network and Information Systems (NIS) Directive. Each of these regulations imposes specific obligations on cloud service providers, ranging from data protection and breach notification to facilitating data portability and ensuring fair market practices.

These are briefly summarised in Figure 3.8 below and in Annex B.4:

Figure 3.8: Summary of key EU regulation applied to cloud services [Source: Analysys Mason, 2024]

Regulation	Summary
Data Act	Facilitates access to and sharing of certain data under certain contractual terms to ensure fairness as well as enhancing portability
Digital Markets Act	Identifies business as 'gatekeepers' of digital services and prohibits unfair practices by these businesses
Digital Services Act	Regulates content moderation, risk management and transparency
Digital Governance Act	Seeks to ensure neutrality and trust, data altruism and re-use of certain protected data
Platform-to-Business Regulation (P2BR)	Seeks to promote fairness and transparency for business users of online intermediation services
NIS and NIS2	Various regulations related to data security and incident reporting
GDPR	Stipulates regulations around data protection and security including rights of access for data subjects
Digital Operational Resilience Act	Aims at strengthening the IT security of financial entities such as banks, insurance companies and investment firms
Artificial Intelligence Act	Regulates high-risk applications of AI, including when deployed on cloud platforms

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

Summary

As discussed in Section 2.3, cloud providers make use of an array of network inputs including private networks (including investments in submarine cables), CDNs and the ability to Interconnect at IP level with ISPs to enable end users to access content and applications hosted in the cloud. These aspects have been mentioned specifically in a recent BEREC report.[113]

Cloud providers' private networks enable connectivity between their data centres and PoPs. In some instances, cloud providers directly invest in submarine cables for this purpose, 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. This is fundamentally different from the provision of capacity for the purpose of public ECS.

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. They do so in part by caching content close to end users, including through 'on-net' caches located in ISPs' premises. Third-party CDNs do not deliver their own content, but rather their customers' content. They do so by handing over traffic to ISPs, which then deliver it to end users who requested it.

IP interconnection between cloud providers and ISPs, or between CDNs and ISPs, is essential to end users' ability to access cloud services. As described in Section 2.3, 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 for the EECC's definition of interconnection, which focuses on traditional telephony. The telecoms regulatory framework specifies interconnection rules, and indeed regulated relevant interconnection markets 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'. This prevents the emergence of the market failures that the EECC's regulation of interconnection for ECS providers addresses.

BEREC has recently found that IP interconnection on the internet has worked, and continues to work well, in the absence of regulation, which appears to be supported by the absence of any significant disputes related to IP interconnection between cloud providers and ISPs in Europe. Overall, this suggests there are no specific characteristics of cloud services that would justify deviation from general IP interconnection regulation for the broader internet.

As discussed in Section 2.3, cloud services interact with telecoms in several ways, most notably because cloud customers must be connected either to the internet or directly to the cloud provider to be able to use those services.

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

In this section, we directly address three aspects of connectivity that have been called out in recent communications by BEREC and the EC (albeit with different viewpoints):

- network links used by cloud providers between their data centres and PoPs
- the exchange of traffic, through IP interconnection, between cloud providers and ISPs
- the use of CDNs and the exchange of traffic between CDNs and ISPs.

3.3.1 Cloud providers' operate their own private networks, carrying traffic between data centres and other PoPs through terrestrial and submarine networks

Cloud providers operate global private networks linking their infrastructure using inputs from many different providers, in a similar way as other large multinational businesses

The use of private networks by cloud providers is identical to how many large multinational corporations (such as banks and airlines) have historically operated wide-area networks (WANs), through a combination of managed services provided by large carriers and service providers (e.g. Orange Business) and of their own network equipment running on lower-level inputs (including dark fibre).[114]

By definition, the data that flows on these networks includes customer data, but importantly the service offered through the use of these networks has nothing to do with the conveyance of signals:[115] banks offer a broad range financial services, airlines provide airplane tickets, cloud providers offer a broad range of IT services including compute and storage.

In the context of cloud providers' private networks, traffic flows between data centres reflect the distribution of resources used for a given service between any number of data-centre locations, and the replication of content and workloads across multiple locations to increase resilience. Although user choices and inputs have an impact on inter-data-centre traffic (e.g. if a user chooses to replicate their data in two specific regions), cloud platforms manage these flows of traffic themselves based on their overall requirements across multiple users. This is similar to how other online services operate, interacting with their customers through the internet and managing their own private networks separately.

Large content and cloud providers have actively invested in submarine capacity, directly or through contractual agreements with submarine cable operators, for use in their private networks

Submarine cables are essential to operating global networks for any organisation running its own WAN. In the majority of cases, submarine cables are commissioned and operated through a

114 See for example Ciena (2017), *A Framework for IP/Optical Convergence: Building from Existing Networks*.

115 We note that this is not fully defined in the EECC. Article 2 ('Definitions') talks about "the conveyance of signals by wire, radio, optical or other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including internet) and mobile networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed".

consortium model, with multiple stakeholders funding, owning and operating part of the cable. In some cases, cables can be private, and in recent years some private cables have been built by large content and cloud providers for their own use.[116]

Data collected by BEREC in a recent report demonstrates different strategies: Google and Meta appear to have been the most active in participating directly in the creation of new cables, with Microsoft and Amazon relying instead on acting as anchor tenants on cables rolled out by other parties.[117] This reflects a typical 'build or buy' decision, which characterises many connectivity services: depending on demand and supply dynamics, a major user of connectivity has a choice to buy services from a commercial provider, or to build its own network. It is worth noting that this trend is not specific to cloud: Meta does not offer public-cloud services, and many other CAPs are buying 'indefeasible rights of use' (IRU) and long leases on submarine cables despite not owning them directly.[118]

Cloud providers do not actively sell capacity on the submarine cables they invest in. They either co-invest with commercial operators, or trade capacity in exchange for services, such as landing and operating the ground segment and landing station of a cable, or through 'swaps' for capacity on other routes.[119] Through these mechanisms, telecoms operators continue to play a central role in submarine cables, even as more investment has flowed from large content and cloud providers.[120]

In all of these cases, cloud providers control the capacity they invest in or lease, using it as an input into their private networks and the services they provide.

Private networks do not currently fall under the scope of the EECC

The EECC defines what constitutes a **public** electronic communications network:

- A **public electronic communications network** is defined as "an electronic communications network used wholly or mainly for the provision of publicly available electronic communications services which support the transfer of information between network termination points." (EECC article 2(8))
- A **network termination point** is defined as "the physical point at which an end-user is provided with access to a public electronic communications network, and which, in the case of networks

116 Dunant, Equiano, Curie and Grace Hopper are all examples of Google private cables, whilst Echo, Apricot, Havfrue are examples of consortium cables in which Google has a stake.

117 BEREC (2024), *Draft BEREC Report on the entry of large content and application providers into the markets for electronic communications networks and services.*

118 See for example *EXA Infrastructure*.

119 See for example TeleGeography (2019), *Is Your Planned Submarine Cable Doomed?*

120 See TelcoTitans.com (2023), *Interview: Orange Wholesale chief says hyperscaler investment, cloud data and AI surge fundamentally changing subsea cable infra.*

involving switching or routing, is identified by means of a specific network address, which may be linked to an end-user's number or name." (EECC article 2(9))

Whilst the scope of publicly available telecoms services is broad, it does not include internal networks which are not provided to third parties (i.e. private networks). This is supported by the reference to network termination points, which are points at which the public can access the public electronic communications network.

Applying the EECC definitions, connectivity used by cloud providers for their own internal use (including submarine cables) are private networks: they are not provided to the public and do not feature network termination points accessible to the public.[121]

3.3.2 Interconnection between cloud providers and public ECS/ECN providers reflects the essential asymmetry between ISPs and any over-the-top content provider

Interconnection regulation has been an integral part of telecoms regulation since its inception to address the specific problems of incumbency and network effects specific to the telecoms sector

As discussed in Annex A, in the EU telecoms regulatory framework, the obligation for regulated telecoms providers to interconnect with one another has been enshrined in law from the start, and remains included in the EECC.

The regulatory obligation to interconnect is designed to address the imbalance between new entrants and incumbents in the telecoms sector derived from network effects and economies of scope, scale and density. Without regulation, there is a significant risk established operators may abuse its network effects by refusing to interconnect with a new entrant, or imposing prohibitive price barriers. In voice telephony markets, this has further translated into the regulation of wholesale voice call termination at EU level until 2020, and the continued imposition of a Union-wide regulation of wholesale call termination prices.[122]

Beyond telephony, which is now less closely intertwined with network access, broader IP interconnection is a very important feature of how the internet works. Indeed, cloud providers and telecoms operators connect in multiple locations, following their own independent strategy: for example, AWS reports over 410 PoPs in over 90 cities across 48 countries,[123] and OVHCloud operates 44 PoPs globally. Europe is also home to 167 peering locations (or 'exchanges' as reported by PeeringDB) across almost all EU countries, as shown in Figure 3.9, which demonstrates the wide distribution of interconnection points used by cloud providers and IT networks more generally.

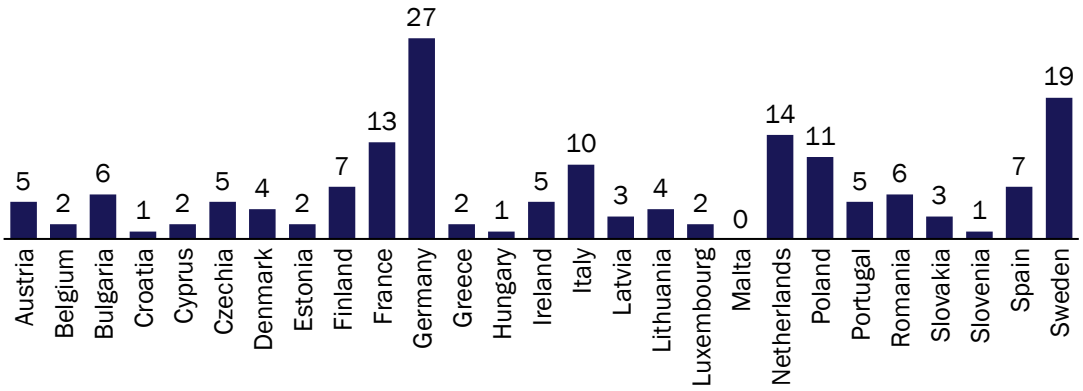
---

121 See also Dean Bubley (2024), *Private Networks: Should They Face EU Regulation? And Does the Commission Know What They Are? - Disruptive Competition Project (project-disco.org).*

122 The EC's Staff Working Document related to the 2014 updated recommendation on relevant market anticipated the impact of IP-based telephony on the inclusion of voice call termination in relevant markets under the regulatory framework. See European Commission (2014), *SWD(2014) 298.*

123 See AWS, *Points of presence* (Accessed July 2024).

Figure 3.9: Number of peering points per EU country [Source: PeeringDB, Analysys Mason, 2024]



These PoPs provide the opportunity for the exchange of traffic between thousands of IP networks on the internet ('IP interconnection', although this is not interconnection under the meaning of the EECC), including ISPs and large customers. Most interconnection arrangements are informal, so-called 'handshake' agreements.[124] Others are framed by commercially negotiated contracts, which are subject to competition law but not ex-ante regulation.

These agreements enable better 'best-effort' connectivity through the public internet, through a set of diverse routes that limit congestion and offer low-latency options. They also enable telecoms operators and cloud providers to partner to offer 'cloud on-ramps' to cloud users, which are dedicated connectivity products sold by operators to those cloud users to avoid the public internet.

There is no clear justification for regulating IP interconnection, including between cloud providers and public ECS providers, under the scope of the EECC

As BEREC states very clearly in its recent consultation paper on the topic, IP interconnection on the internet has worked, and continues to work very well in the absence of regulation.[125] This is in stark contrast with legacy interconnect between ECS providers of end-to-end interpersonal communication services not using the internet where high pricing and exclusionary practices emerged, requiring regulatory intervention.[126]

Specifically, IP interconnection between cloud providers and ISPs, and between CDNs and ISPs, appears to be functioning well. We are not aware of IP interconnection disputes involving cloud providers, and where IP interconnection disputes have occurred, they have tended to involve ISPs foreclosing access to end users. We have addressed this in a 2022 paper, and others have observed

124 Packet Clearing House conducts a broad survey of peering agreements every five years. The latest survey, from 2021, surveyed over 15 million agreements, covering over 17 000 carrier networks around the world. It found that 99.998% of these agreements were informal handshake agreements. See Packet Clearing House (2021), *Survey of Internet Carrier Interconnection Agreements*.

125 BEREC (2024), *BEREC Report on the IP Interconnection ecosystem*: "Generally, the IP-IC ecosystem is still driven by competitive forces which are functioning without regulatory intervention." (p.37).

126 See, for example, Arcep (2017), *Draft decision 2017-xxxx*.

similar dynamics.[127] This suggests that there is no unique characteristic of cloud services that would justify regulating IP interconnection on the internet.

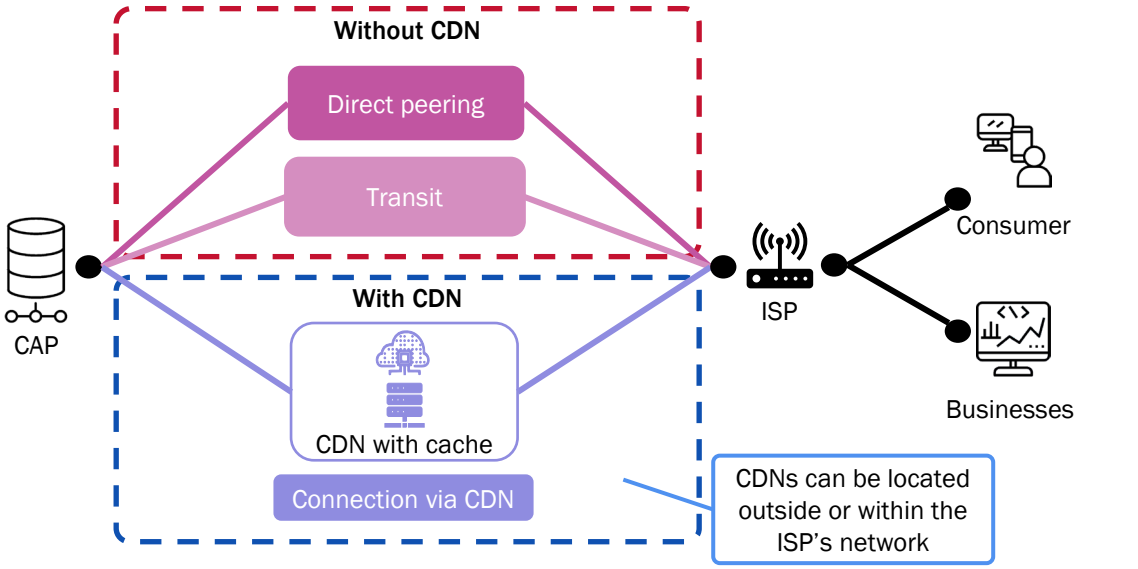
In Section 4, we explore the potential impact of taking an expansive approach to regulating IP interconnection, based on statements of intent by some large operators.

3.3.3 CDNs store and serve online content close to end users, optimising quality and cost to the benefit of end users, content providers and ISPs

As introduced in Section 2.3.2, CDNs are services used by online content providers in order to optimise the delivery of their content and services to end users. CDNs are particularly useful when content needs to be delivered in multiple locations, to many ISPs, in the most direct way possible.

CDNs store content in decentralised servers, often located in PoPs where they interconnect with ISPs, or directly in ISPs' premises ('on-net CDNs').[128] ISPs work with CDNs as a way to reduce the costs of collecting traffic requested by their customers (internet and cloud users), by interconnecting directly with CDNs in locations where they themselves already operate PoPs (internet exchange points, private peering facilities, or directly within their network nodes for embedded or on-net caches).[129] This is illustrated in Figure 3.10.

Figure 3.10: Content provider approaches to CDN [Analysys Mason, 2024]



127 See Analysys Mason (2022), *IP interconnection on the Internet: a European perspective for 2022*; WIK (2022), *Competitive conditions on transit and peering markets.*

128 See for example *ITU-T F.750 Metadata framework* and BEREC (2024), *Draft BEREC Report on the entry of large content and application providers into the markets for electronic communications networks and services (europa.eu).*

129 See Analysys Mason (2022), *Netflix's Open Connect and codec optimisation saved ISPs over USD1 billion (analysysmason.com).*

CDNs also provide services that improve the quality, security and resilience of their customers' online presence. For example, they can handle content requests on behalf of a specific content provider's own network, to optimise how the content is served, balance the loading on different cache locations, and mitigate some forms of congestion, including denial-of-service attacks that seek to overload specific networks as a form of cyber offence.[130]

Whilst CDNs certainly use electronic communications as an integral part of how they operate, they do not "consist wholly or mainly in the conveyance of signals".[131] CDNs also involve the storage of content in multiple locations, and the optimisation of the delivery of content based on decisions taken by the CDN, its customers (content providers) and ISPs. BEREC found that CDNs were mostly used to direct traffic from content providers to end users, demonstrating the close link between CDN and content (as opposed to networking per se).[132]

European jurisprudence provides some indication of how the courts would consider the question of whether CDNs could be classified as ECS (see Annex B):

- A CDN does not involve editorial responsibility: the CDN provider simply stores and permits access to content provided by its customers i.e. the content providers.
- A CDN provider has no responsibility to the end users with respect to conveyance of signals – instead its responsibility is towards the content provider, but that responsibility is defined in terms of the latency experienced when content is access, not primarily for the conveyance of signals.
- For the reasons described above, the provision of a CDN does not consist "wholly or mainly in the conveyance of signals on electronic communications networks".

On this basis, it is likely that European courts would consider CDNs as falling outside the scope of electronic communications services. Furthermore, in the absence of a clear problem or market failure associated with CDN providers, regulating CDNs under the EECC is unlikely to be justified, proportionate, or aligned with the purpose of the telecoms regulatory framework.

130 See for example Cloudflare, *Distributed denial-of-service (DDoS) protection* (Accessed July 2024).

131 For the avoidance of doubt, they also do not offer internet access services or interpersonal communications services, as per recital 15 of the EECC.

132 BEREC found that that about seven times as much traffic flows from CDNs to ISPs as in the other direction. See BEREC (2024), *BEREC Report on the IP Interconnection ecosystem.*

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

The EC's proposal to extend telecoms regulation to cloud providers can be seen as part of a broader industrial policy objective, to develop what the EC calls "connected collaborative computing", a broad vision that encompasses connectivity, cloud, semiconductors and data.

As discussed in Section 3, there is no established problem or market failure that would justify applying the telecoms regulatory framework to cloud services. Indeed, the telecoms regulatory framework has not been designed to address dynamics at play in the cloud sector, and would not be well suited to remedy cloud-specific competition concerns in a proportionate way. Expanding regulation to achieve industrial policy goals would require detailed justification and an impact assessment. It would also need to conform to established principles of EU law, including justification, proportionality and the respect of fundamental rights.

In this section, we provide initial thoughts on the potential consequences of bringing cloud services under the telecoms regulatory framework. We have considered the impact on cloud providers and customers, telecoms operators and their customers, and the broader digital agenda for Europe.[133]

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. This is consistent with the views expressed by many stakeholders in response to the consultation on the EC's white paper,[134] with the notable exception of the largest telecoms operators, which have long been arguing for regulated interconnection and material monetary transfers from online content providers, including through cloud and CDNs.[135]

Finally, such an expansion of complex regulation would go against the key objectives of the new European Strategic Agenda,[136] including "remain an attractive location for investment", "boosting Europe's capacity in enabling and emerging technologies" and "reduce the bureaucratic and regulatory burden at all levels".

133 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).

134 See for example Internet Society (2023), *"Fair Share" Proposal in the EU*.

135 ETNO (2023), *9 questions and answers on the "fair contribution" debate*.

136 European Council (2024), *Strategic Agenda 2024-2029*.

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

Summary

If the European telecoms regulatory framework were expanded to include cloud and CDN services, the providers of these services would face additional cost and complexity in operating in Europe. The direct costs associated with authorisations and compliance may be manageable, but 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 scale that characterise it. It is at odds, however, with the cross-border nature and economies of scale of cloud and CDNs, which are recognised in the EU 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.

In addition, 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 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.

Similar cost, complexity and uncertainty would stem from the inclusion of cloud and CDN providers' private networks under the EECC. Its purpose and construction have very clearly distinguished between public ECSs and ECNs, which it oversees, and private networks, which are not subject to regulation. Changing this for cloud and CDNs specifically risks bringing private networks more generally under the regulatory framework, with no clearly established justification.

Overall, these effects would increase cost, complexity and risks for cloud and CDN providers. This could discourage further investment, and reverse recent trends towards more decentralised infrastructure (both cloud regions and PoPs). Smaller Member States could be most affected, as demand for cloud and CDNs may be insufficient to justify providers being regulated in one more country. Ultimately, the European businesses that use cloud and CDNs (including European CAPs) would face higher cost and lower-quality services as a result.

4.1.1 Cloud and CDN providers would face complexity and costs at national as well as EU levels, at odds with a business model that benefits from cross-border economies of scale to users

The extension of the telecoms regulatory framework to cloud services will generate additional costs for all cloud providers, including administrative and staff costs, compliance systems and processes, and additional legal fees.[137] These costs would be in addition to those required to comply with recent

[137] See for example OECD (2014), *OECD Regulatory Compliance Cost Assessment Guidance*.

EU-level regulations such as the Data Act and other regulations outside the telecoms framework, as there is no explicit link between these regulatory instruments.

Under the current telecoms regulatory framework, individual NRAs enforce the rules at the national level, with harmonisation at the EU level happening subsequently. Although compliance costs per se may be manageable, the complexity associated with national-level regulation, which persists under the EECC, would create significant frictions in the cloud sector. There is no clear justification for why cloud regulation should be national in scope, and existing regulations that do apply to cloud services (including the Data Act and the Digital Services Act) are EU-wide in nature, even where some enforcement may occur at Member State level.

Furthermore, the economics of the cloud sector show the benefits of economies of scale across borders: customers are able to use infrastructure that is located anywhere in the world, subject to sovereignty requirements and good international connectivity. Cloud providers and customers benefit from economies of scale and scope that are not bound by national borders, in contrast with telecoms, where economies of scale are primarily local.[138] The national application of rules to a sector that is by nature global would likely deter cloud providers from entering new markets if this makes them subject to a different set of obligations vis-à-vis new NRAs.

Size will be a differentiator of impact among cloud providers, with larger players likely to be better able to cope with the added compliance burden. This could be counterproductive to competition in the European cloud sector, and deter entry by new providers. In the context of the EC's desire to bring about more European cloud infrastructure and services, the complexity and costs associated with regulation are likely to make market entry and expansion for these European players more complicated. One exception may be large established telecoms operators: although their cloud activities are not covered by the EECC, the additional cost and complexity may be limited.

4.1.2 The inclusion of cloud providers and CDNs under the EECC could lead to regulated IP interconnection and private networks, increasing complexity and costs

Mandating interconnection and dispute resolution between cloud and CDN providers, and telecoms operators, would effectively make IP interconnection a regulated service

The telecoms regulatory framework may impose a mandatory requirement for cloud providers to interconnect with network operators, subject to the dispute resolution mechanism specified in the EECC. This would extend the definition of interconnection to include IP interconnection, rather than the traditional telephony interconnection and associated network effects that the EECC is designed to address, as discussed in Section 3.2.

The introduction of mandatory arbitration could lead to large network operators engaging in disputes with cloud providers to solicit higher peering or transit fees. This seems a likely outcome, because

138 This is the reason why cross-border consolidation of telecoms operators in Europe has not gained more momentum: there is no strong cost or revenue benefit in doing so due to the localised nature of economies of scale.

of the extensive lobbying by some of the largest telecoms operators to introduce a mandatory dispute resolution process as a way to put pressure on CAPs (including cloud and CDN providers) to pay more for interconnection with ISPs (the so-called 'fair share' argument). Indeed, an ETNO-commissioned report highlighted the potential for 'direct compensation' through this process, referencing estimated annualised costs of EUR36–40 billion incurred because of internet traffic.[139,140]

Although there is significant uncertainty associated with such dispute resolution, it may result in three types of outcomes:

- One outcome would be the ISPs pay cloud providers, for example if regulators take the view that cloud providers' investments in caches and CDNs result in a net benefit for ISPs, which they should compensate cloud providers for.
- A second outcome may be that regulators conclude the current arrangements work well, and resolve the dispute by enforcing the status quo.
- The third possible outcome is that dispute resolution leads to a transfer of funds from cloud providers to ISPs through the introduction of traffic termination fees payable to ISPs.

The outcome would only become clear once disputes are brought to NRAs, which will then need to analyse the situation and arbitrate accordingly, likely at a national level, based on their views of the economics of traffic delivery.[141]

As discussed in Section 3.3.2, BEREC and others view IP interconnection as functioning well, and the few disputes that arise tend to be related to incumbent network operators abusing a strong position in broadband access markets.[142] Regulating IP interconnection would therefore not solve a clearly identified issue, and would be a significant departure from how the internet has developed over the last forty years, based on unregulated interconnection agreements between thousands of networks, according to their individual incentives and priorities.

The consequence of such an approach would be significant complexity and costs associated with regulation, for no clear benefit. Furthermore, as explained by proponents of regulating IP interconnection including ETNO, this would not only affect cloud and CDN providers, but all the

139 Axon Partners (2022), *Europe's internet ecosystem: socio-economic benefits of a fairer balance between tech giants and telecom operators*.

140 Frontier Economics (2022), *Estimating OTT traffic-related costs on European telecommunications networks*.

141 Analysys Mason has been involved in dozens of market review processes in the context of mobile and fixed call termination markets under the 2002 EU framework. These are individually complex, lengthy exercises that were justified by the scale of distortion to competition and consumer prices from materially above cost mobile termination rates in particular. Once those distortions became less material, the EC imposed a unique price ceiling throughout the EU via a 'delegated regulation', specifically "in order to reduce the regulatory burden in addressing the competition problems relating to wholesale voice termination consistently across the Union". See recital (1) in European Commission (2021), *Commission Delegated Regulation (Eu) 2021/65*.

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

CAPs that use cloud services, and the millions of European businesses and consumers that access content and applications online.

Regulating cloud and CDN providers' use of private networks would suggest bringing all private networks under the EECC, in contradiction with the purpose and goals of the regulatory framework

Cloud providers pool compute, storage and networking resources in a distributed architecture to offer their services. Being able to carry data between all their data-centre locations is a core requirement of cloud providers' operations, as is being able to connect these locations to interconnection PoPs (e.g. IXPs, peering points and transit providers).[143]

As described in Section 3.3, these are private networks, controlled by cloud providers to manage a global, large-scale decentralised infrastructure. If the EC decides to classify cloud-related private networks as public ECNs, because they carry cloud customers' data, it may have to expand this to any CAP that uses its own network to carry or store user-generated content, including social media platforms, photo and video storage websites, and potentially any business providing services over the internet using in part its own private network.

This would be at odds with the purpose and goals of the telecoms regulatory framework, which specifically focuses on electronic communications services offered to the public. Trying to separate private networks between regulated and unregulated ones would create uncertainty and costs, including through litigation.[144]

4.1.3 Cloud providers and CDNs may reduce their investments in European digital infrastructure as a result, to mitigate risks and costs

Increased compliance costs and interconnection fees could reverse ongoing trends towards more decentralised cloud and peering infrastructure, especially for smaller Member States

As mentioned above, the imposition of national regulation and enforcement under the EECC to the cloud and CDN sectors could act as a deterrent for cloud and CDN providers to enter new European countries, in particular smaller ones, if they can operate from a small number of larger Member States. This would reverse the ongoing trend towards more decentralised cloud regions, which responds to demand for low latency and high service quality, and to data sovereignty requirements (e.g. for public-sector cloud users) that are specific to Member States.

143 See Figure 3.10.

144 The definition of ECS and ECN has already be the subject of significant legal disputes at national and EU levels. For example, in 2016, the Belgian NRA (IBPT) fined Skype for failing to notify its SkypeOut service as an ECS. The case was litigated, including in the European Court of Justice, which found in favour of IBPT in 2019. See ECJ (2019), *Judgement of the Court in Case C-142/18*.

The second trend that could be reversed as a result of the expansion of the telecoms regulatory framework to cloud and CDN providers would be the growth in decentralised IP interconnection and direct peering.

In the absence of regulatory hurdles, cloud providers seek more direct interconnections with local network providers, preferring public and private peering over transit.[145] While transit requires low initial investment, prices charged are typically based on used bandwidth. Conversely, peering allows two networks to exchange traffic directly, only limited by the investment in interconnection capacity between their two networks. As they grew, cloud and CDN providers have invested significantly to build presence and capacity to deliver their traffic closer to ISP networks, improving the user experience of cloud-hosted services.[146] As networks peer more, they reduce their reliance on transit, lowering costs and improving performance.

In response to interconnection regulation in the EU, cloud and CDN providers may opt to only offer peering outside the EU. Telecoms operators that currently interconnect with cloud and CDN providers domestically would have to do so internationally, or rely on transit more. A shift to alternatives to peering would reduce quality and resilience of European internet infrastructure and increase costs throughout the internet ecosystem, including for cloud and CDN providers, telecoms operators, and European businesses and consumers. This could also be counterproductive to the EC's objectives to make Europe less dependent on other regions, if peering moved outside the EU as a result.

Third-party CDNs would also be directly affected, leading to higher costs for businesses that rely on them and putting at risk the benefits they bring to the internet ecosystem

BEREC's report comments that "technological developments, such as the installation of on-net CDNs, are a key reason why increases in data traffic have not filtered through to prices and costs."[147] A regulatory shift towards paid peering could potentially reverse these positive trends.

If network operators were to require compensation from CDNs for peering, it might undermine the efficiencies achieved through unmetered peering and on-net caches. In this scenario, traffic could be subject to paid peering regardless of whether it is delivered on- or off-net, disregarding the current benefits of local content delivery. This would lead to increased costs for CDN providers, CAPs and consumers, and poorer user experience from increased latency and congestion as CDNs become more centralised.

Importantly, this would undermine the business model of commercial third-party CDNs. As recognised by all parties, including large European telecoms operators that have been advocating for mandated arbitration of IP interconnection between CAPs and ISPs, CDNs are intermediaries:

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

146 Analysys Mason (2022), *The impact of tech companies' network investment on the economics of broadband ISPs*.

147 BEREC (2024), *Draft BEREC Report on the IP Interconnection ecosystem*, Section 4.5.

they act on behalf of CAPs, their customers, which control the content that is handled by CDNs. As a result, CDNs do not have the ability to modify the content, including encoding or compressing it more to reduce their costs.

In South Korea, the imposition of a 'sending party network pays' model (SPNP, similar to what ETNO has been advocating for in the EU) has led some CAPs to cease to interconnect in the country, or even withdraw their services. [148] This shows how higher costs for peering may result in CDN providers reducing their investments in edge caches and PoPs, or even withdrawing from some markets. As for cloud providers, this would result in higher costs for the whole internet ecosystem, including telecoms operators and the businesses that rely on CDNs, including European CAPs and broadcasters.

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

Summary

Reduced investment by cloud and CDN providers would result in more centralised interconnection, which could increase costs for telecoms operators. In addition, if cloud and CDN providers were included under the scope of the EECC, they would face fewer barriers from providing connectivity solutions directly, without needing to partner with ISPS (e.g. cloud on-ramps). They could also choose to operate submarine cable landing stations themselves, without partnering with telecoms operators.

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.

Furthermore, a shift from decentralised peering to greater use of transit, whilst detrimental to many smaller ISPs, could be beneficial to the largest operators with large transit operations. These operators may be able to leverage their larger networks to favour their own CDN and even cloud services, in contradiction with policy efforts to reduce self-preferencing in digital markets including through the Digital Markets Act.

Beyond the impact on cloud and CDN providers and infrastructure, an expansion of the telecoms regulatory framework to include cloud and CDN could result in distortions to the telecoms sector itself, through:

- higher costs and reduced collaboration with cloud and CDN providers
- competitive imbalances as larger operators benefit more from interconnection charges imposed on cloud and CDN providers

148 See for example Korea Herald (2019), *Facebook wins court battle over network cutoff*; Twitch (2023), *An update on Twitch in Korea*; and Carnegie Endowment for International Peace (2021), *The Korean way with data*.

- larger telecoms operators promoting their own cloud services in ways that could be detrimental to competition and to consumers.

4.2.1 Reduced network investment by cloud and CDN providers could increase costs and reduce revenue opportunity for operators

As explained in Section 2.3, the cloud sector is dependent on the ability of cloud providers and customers to connect to one another, through cloud on-ramps or through the internet. Telecoms operators facilitate connectivity between cloud providers and their customers through internet access services and dedicated connectivity solutions. They also work with cloud providers to deploy and maintain edge infrastructure and sovereign cloud solutions. Finally, cloud providers purchase private network links from operators, and rely on them to land capacity on the submarine cables they invest in.

Should cloud providers find themselves being regulated under the telecoms framework, these partnerships may be negatively affected:

- Cloud providers could decide to move into providing connectivity themselves, since they would already be affected by the associated regulatory framework already. This could include on-ramps and multi-cloud networking.

- Cloud and CDN providers that invest in submarine cables and rely on telecoms operators to land capacity in the EU may decide to do so themselves. This would reduce the opportunity for operators to access capacity on these cables without investing directly in them.

- Other strategic relationships between cloud providers and telecoms operators may be negatively affected by disputes, including on interconnection, to the detriment of both parties. This could include sovereign cloud services[149] that regulated cloud providers may be able to offer themselves.

This could result in Europe becoming more, rather than less, dependent on global cloud providers, despite the EC's stated objectives to use industrial policy to favour the emergence of European cloud providers.

4.2.2 Large operators may benefit disproportionately from 'network fees', distorting competition with smaller operators

In the event that interconnection disputes result in financial transfers from cloud and CDN providers (and other CAPs) to telecoms operators in the form of network usage fees, larger operators would secure a significant share of these transfers of funds, due to their larger number of subscribers.

These subscribers request internet content from CAPs, many of which use cloud services. If the arbitrated rate at which these transfers occur is above marginal costs, these transfers could distort

149 See for example TM Forum (2024), *Sovereign clouds roll in to Europe*.

the competitive balance between smaller and larger telecoms operators, by concentrating monetary flows to the latter. This seems likely given many larger operators have been supportive of the prospect of 'network fees', while their smaller peers have highlighted the competitive risks.[150]

Reduced competition between telecoms network operators would likely further diminish incentives for infrastructure investment, as dominant players would face less pressure to improve their services. These companies might instead focus on legal strategies to increase network fees, potentially resulting in higher consumer costs driven by a less competitive landscape and stagnating technological progress. As exemplified in several European countries, competition from alternative providers can spur investments from incumbent operators.[151] Consequently, a reduction in competition will not contribute to such incentives.

Finally, a shift from domestic or local peering to transit, in the event that IP interconnection becomes more centralised, would result in increased demand for transit and international connectivity to peering hubs. The main providers of these services are large incumbent telecoms operators, which further benefit at the expense of other stakeholders. This would distort competition between network operators by concentrating traffic to a smaller number of players and reduce the opportunity for smaller operators to offer key growth networking services such as multi-cloud networking.

4.2.3 Some telecoms operators may exploit these changes to promote their own cloud services, at the expense of European businesses and cloud providers

As explained in Section 2.2.2, some telecoms operators are already participating in the cloud sector. These services are not currently covered by the EECC and other telecoms regulation, but could be regulated if the EECC were expanded to include cloud services. The EC appears to see this as a way to 'level the playing field' between cloud providers and telecoms operators, in the provision of cloud services in the EU.

This seems unlikely to enhance the incentives or capabilities of telecoms operators to provide cloud services, unless they could explicitly leverage their position as both ISPs and cloud providers to gain a competitive advantage over cloud-only providers. This could happen if they were allowed to price inbound IP interconnection well above cost and use these profits to compete on price with cloud providers on cloud services.

This sort of cross-subsidy from termination monopolies is exactly what the regulation of call termination rates was intended to reduce. It could also give rise to self-preferencing by telecoms operators of their own cloud and CDN services, despite efforts to prevent such self-preferencing by

150 See for example the joint statement published by ETNO (2021), *Europe needs to translate its digital ambitions into concrete actions*, and discussion on impacts of 'network fees' by Association des Opérateurs Télécoms Alternatifs (2022), *There cannot be a functional Internet for those who pay and a second-rate Internet for the others.*

151 For example "The dearth of infrastructure competition gave Openreach no market incentive to invest in full-fiber networks. [...] The UK was stuck at the bottom of European full-fiber rankings", LightReading (2022), *Despite critics, fiber rollout is a rare UK success story*. or OECD (2015), "*Development of High-speed Networks and the Role of Municipal Networks*".

large providers under the Digital Markets Act.[152] Both of these could lead to market failures and harms to consumers and competitors, including smaller telecoms operators and other cloud providers.

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

Summary

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 concerns expressed by a range of stakeholders in response to the EC's consultation on the white paper reflect the breadth of negative impacts that would stem from the EC's proposals. 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.[153] This would slow the adoption of cloud services and innovations including AI, going against the EC's efforts to spur digital transformation under its digital agenda. 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 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.

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.

152 See for example CERRE (2022), *The prohibition of self-preferencing in the DMA*.

153 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)

4.3.1 European businesses and CAPs will suffer from more expensive cloud services and reduced access to innovative digital tools, in contradiction with the goals of the digital agenda

European businesses may be affected by higher costs for cloud services, and less choice for both cloud and networking services

For European businesses that use cloud services, greater costs for cloud providers driven by increased regulation may negatively affect cloud adoption through three routes:

- **Increased prices for cloud services**. As indicated by major cloud providers in their responses to the EC white paper consultation, higher costs for cloud providers may lead to increased prices for cloud services.[154] This could result in reduced usage among larger businesses with sophisticated IT departments, which might opt to self-supply. Smaller businesses might decide against adopting cloud services altogether.

- **Reduced innovation, quality and service availability due to re-allocation of resources**. Cloud providers may divert resources from investments and innovation to cover increased regulatory costs. This reallocation could degrade the quality of services for end users by a slower rate of innovation and infrastructure build-out by cloud providers further incentivising businesses to reduce usage or self-provision. Furthermore, cloud providers could decide not to launch specific services in the EU, if the regulatory costs and complexity outweighed the potential benefits they would derive from these services.

- **Reduced competition and choice due to higher barriers to entry**. Competition in the cloud sector may be reduced as existing providers may reconsider expansion into new markets and prospective entrants may focus elsewhere in light of a more challenging and fragmented regulatory landscape. This would affect the choice and quality of services available, further impacting cloud service adoption and ultimately the growth of the sector. Smaller businesses would see heightened impact of such developments due to their limited ability to self-provision.

Additionally, reduced competition in the telecoms sector could lower the choice and quality of networking services available to European businesses.

Slower cloud adoption by European businesses would be detrimental to the digital agenda, reducing take-up of technology including AI and data-driven innovations that could foster competitiveness

Reduced access to services due to cloud providers withdrawing or not launching services will similarly affect end users as they will either have to invest to provide services themselves or be faced with less choice from remaining providers. This could entail slowing or reducing the scale of digitalisation for European businesses, and the emergence of digital-first start-ups, negatively affecting the competitiveness of the regional business sector.

154 See for example response from Google, available at European Commission, *How to master Europe's digital infrastructure needs?* (Brussels, 2024, COM(2024) 81 final).

Beyond European businesses, the public sector, including government, education and healthcare, will also need to allocate more resources to cloud services and may face a reduced choice of services affecting its digitalisation.

Organisations in smaller Member States are particularly vulnerable, as the limited incentive to launch local services combined with the risk of stringent regulations from additional NRAs will drive cloud providers to focus on larger markets.

Overall, this would go against the objectives of the European digital agenda, which emphasise take-up of cloud services, 'big data' and AI as drivers of European competitiveness. European businesses active in digital technology would be particularly affected, including European CAPs and broadcasters, which will face increased costs for using cloud and CDN services.

4.3.2 The higher risk, costs and complexity for cloud and CDNs providers of investing in Europe will lead to more centralised and less resilient digital infrastructure

The reversal of recent trends towards more decentralised internet infrastructure would come at a financial cost, but would also be detrimental to the resilience and security of European digital infrastructure. This could result from:

- greater reliance on transit, which would create a less interconnected and less resilient internet
- disincentives for cloud providers to deploy infrastructure in more Members States, due to the risk of national regulation
- less collaboration between telecoms operators and cloud providers and other CAPs in the context of new submarine cables.

CAPs (including cloud providers) have been increasingly active in international connectivity, transitioning from being buyers of capacity to investing in the deployment of new cables to support their local data centres with the connectivity they require. BEREC notes that "[t]his is in general beneficial for Europe in terms of investment, as well as data sovereignty, as more data is stored and processed in Europe rather than in third countries".[155] It also improves diversity in submarine cable routes and landing, which improves the resilience of Europe's international connectivity.

If their investments in submarine cables brought them under the telecoms regulatory framework, cloud providers could have lower incentives to invest in submarine cables directly. They would have other options, such as committing to long leases and 'indefeasible rights of use' (IRU) for the whole life of the cable, before the cable is even built. This would result in lower direct investment by cloud

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

providers, and higher investment by traditional telecoms operators. It may also result in poorer outcomes for cloud providers, with slower technology innovation[156] or cable deployment.[157]

An alternative would be for cloud providers to spin off their submarine cable investments into separate entities, which will be subject to regulation. This will have no direct impact on cloud providers but may result in fewer opportunities for telecoms operators to access capacity on new cables: these new entities would be able to secure the national licences needed to establish landing stations for international submarine cables themselves, rather than rely on existing partners to land the cable.[158]

We note that BEREC's recent work on submarine cables include suggestions to improve incentives for multiple parties to continue investing in submarine cables that land in Europe. These include measures to improve the security and protection of submarine cables, more harmonised and co-ordinated approach to obtain landing permits, and encouraging more diversity in submarine cable routes. An approach that reduces incentives to invest, or to partner to make submarine capacity broadly available, would go against these broadly consensual objectives, leading to scarcer, less resilient and less secure digital infrastructure and global connectivity for Europe.

4.3.3 Expanding the telecoms regulatory framework to the cloud sector for industrial policy reasons, without clear justification or impact assessment, would increase regulatory risk

The lack of clear justification and impact assessment in bringing cloud services under the EU telecoms regulatory framework would create regulatory uncertainty. This may lead cloud providers to 'over-comply' for existing services to avoid disputes, incurring both direct and opportunity costs.[159] The application of unclear regulation may cause sector participants to implement more stringent internal policies than required, conducting more frequent or extensive audits and assessments, or applying stricter standards across all operations, even in jurisdictions with less demanding regulations. The associated costs would be especially susceptible to aspects of the framework which are subject to national differences, such as through market reviews.

More broadly, the success of the telecoms regulatory framework in helping bring about a dynamic, competitive telecoms sector over the last 25 years is a good example of how the principles of EU law benefit European businesses and consumers. Legislation and regulation designed and

156 For example, Google inventing a 12 fibre-pair space division multiplexing design, designing one of the first cables to implement spectrum sharing technology on the terminal side or implementing an overlapping filter-based optical add/drop multiplexer based on Google patented technology.
Analysys Mason (2020), *Economic impact of Google's APAC network infrastructure.*

157 DCD (2021), *Submarine cables find new impetus under hyperscalers.*

158 See TelcoTitans.com (2023), *Interview: Orange Wholesale chief says hyperscaler investment, cloud data and AI surge fundamentally changing subsea cable infra.*

159 The unnecessary burdens of complex regulation are widely recognised and a driver of the EC's "Better Regulation" agenda.
see European Commission, *Better Regulation: why and how (Accessed July 2024).*

constructed for a specific purpose, implemented where justified in a proportionate way, have been essential to this success.

Applying the EU telecoms regulatory framework to cloud services may also be inconsistent with the principles of equality before the law: the telecoms and cloud sectors are fundamentally dissimilar in their market dynamics, historical context and regulatory needs. Treating them identically under the same regulatory framework lacks a fundamental objective and fails to recognise the unique characteristics of each sector. Finally, imposing onerous regulatory obligations (e.g. associated with interconnection) on cloud and CDN services (without clear justification) risks restricting rather than furthering free competition, which may not protect the rights and freedoms of enterprise of these providers.

In summary, expanding the telecoms regulatory framework to cloud and CDN providers, without a clear and agreed purpose, problem statement or impact assessment, is inconsistent with these principles, and will create regulatory uncertainty, rather than the 'level playing field' that the EC argues for in its recent white paper. This would be detrimental, not beneficial, to the EU digital agenda and the future of its digital infrastructure.

5 Conclusions

Any consideration to extend the telecoms regulatory framework to cloud services would demand scrutiny aligned with the core EU principles of necessity and proportionality. It is essential that it reflects the purpose for which the telecoms framework was created, and responds to a proven need within the cloud sector in a proportionate manner.

The history, purpose and structure of the telecoms regulatory framework, enshrined today in the EECC and the role of NRAs, reflect a history of national monopolies, high and non-transitory barriers to entry, and the continued need for regulation in specific aspects such as fixed infrastructure access and interconnection. This has been remarkably successful in enabling market entry by new operators, increasingly bringing advanced connectivity to all Europeans, and ensuring competitive prices.

Despite their complementarity, cloud services and telecoms networks exhibit clear and pervasive differences that extend beyond the nature of the services. The cloud sector is nascent, dynamic, location independent, and lacks significant direct network effects, whereas the telecoms sector is mature, stable, location specific, and has historically been marked by substantial network effects.

The telecoms regulatory framework was not designed to address issues that exist or may arise in the cloud sector, and remains ill-suited to do so. The competition and consumer protection challenges addressed by the telecoms framework are not applicable to the cloud sector. The ex-ante regulatory tools of interconnection (introduced to address network effects) and onerous product market regulation (through a process of identifying and analysing relevant markets followed by the imposition of intrusive remedies) are tailored to a sector offering fundamentally different products, from a different historical context, and exhibiting very different sector dynamics. Competition law applies to both telecoms and cloud services, and whereas the characteristics of the telecoms sector have shown the need for additional ex-ante regulation, the same is not true for the cloud sector.

Forcibly bringing cloud services under the telecoms regulatory framework would risk stifling growth, innovation and competition in the cloud sector and disrupt the competitive balance among telecoms operators, favouring larger ones. This may ultimately affect users of both sectors in the form of higher costs and reduced service choices. It would go against the goals of the Digital Single Market by challenging the establishment of cross-border services, and it would have a disproportionate impact on smaller European businesses using digital services.

Both the cloud and telecoms sectors are crucial to the digitalisation of European private and public sectors and the continent's overall competitiveness. Regulators should acknowledge the potential adverse impacts of overextending the telecoms framework to encompass cloud services. 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.

Annex A A short history of the European telecoms regulatory framework

A.1 The telecoms sector in Europe evolved from state-owned monopolies to a competitive market with many different operators offering a variety of services

The liberalisation of European telecoms transformed a sector dominated by state monopolies into a competitive landscape. The underlying policy rationale for liberalisation was threefold:[160] to foster the creation of a competitive market wherever feasible, to safeguard consumers' interests, and to establish an environment conducive to efficient and timely investment in infrastructure and services over the long term. Regulation took into account the historical context of state-owned monopolies and acknowledged the need for progressive market opening by lowering barriers to entry:

- First, efforts to foster a 'single market' at EU level required market access across the EU, so that providers operating in one Member State could operate in another. The telecoms sector was granted a special status under single-market instruments, allowing individual Member States to control the pace and scope of market opening in order to ensure former state monopolies ('incumbents') could adjust progressively to competition. European directives ultimately imposed full liberalisation and a common set of rules.[161]

- Second, European policy makers saw liberalisation and 'market forces' as a means of keeping pace with advancements in technology. Traditional monopoly providers, often structured and run as public administrations rather than for-profit corporations, were perceived as being unable to keep pace with innovation in technology. In a globalising economy wherein digital technology was (and still is) playing an increasingly central role in competitiveness, European businesses needed to have access to state-of-the-art telecoms services at fair prices.[162]

- Third, European policy makers and NRAs progressively charted and implemented a course from monopoly to a competitive market, which combined active regulation of interconnection between providers and access to the infrastructure of operators with 'significant market power', which led to a gradual improvement in competitive conditions.

This progressive opening of the EU telecoms sector through harmonised EU regulation started with the EC's 1987 Green paper, followed by the 1993 Council of Ministers decision to liberalise the EU's voice telephony markets by 1 January 1998. Rapid sector development followed over the

160 Erkki Liikanen, *The European Union Telecommunications Policy*, presentation delivered at Telecommunications Seminar in Sarajevo, Bosnia and Herzegovina, 2001–07–16.

161 European Commission, *Europe's Liberalised Telecommunications Market – A Guide to the Rules of the Game*.

162 Erki Liikanen, Member of the European Commission, responsible for Enterprise and the Information Society, 2001.

following ten years. Telecoms markets were progressively opened up to competition, and regulation was largely harmonised across the EU, albeit with some national variations in detail and outcome.

The market structure that resulted from this progression includes a combination of infrastructure and service providers. Wholesale access regulation[163] enabled the entry of service providers with limited network assets to offer retail services to end users. Regulators in Europe adopted different approaches to this regulation, to reflect their own national specificities and regulatory objectives.

In recent years, physical network infrastructure (i.e. mobile towers, ducts and fibre optic cables) has been made available as a separate input, but telecoms operators have been (and many remain) mostly vertically integrated.

A.2 The regulatory framework evolved to overcome high barriers to entry, focusing on competitive bottlenecks, such as network access, licensing and interconnection

Establishing a telecoms network involves substantial investments in physical infrastructure such as fibre optics, cell towers and spectrum licences. This is reflected by the fact that network capex accounts for over 90% of an operator's total capex, 60% of which relating to direct investments in infrastructure.[164] At the same time, the payback period of deploying a network is relatively long, with the financial and technical lifetime of passive assets (ducts, mobile towers) expected to last for 20–30 years.[165] The long payback periods and high initial costs limit the entry of new competitors, contributing to the stability of the telecoms sector. For mobile networks, the barrier to entry rooted in initial investment is exacerbated by the fact that spectrum is a scarce resource, which is awarded for long periods of time (typically 15–25 years,[166] but up to 40 years in some European countries)[167] to individual operators at significant cost, driven in many cases by competitive auction processes.

Traditional telephony services (such as voice calls and SMS) are integrated with the underlying network. This means that calls made between end-user customers of different networks require those networks to interconnect and agree charges for the conveyance and termination of those services. Network effects, exacerbated by sunk costs and economies of scale, scope and density made market entry difficult without ex-ante regulation of interconnection and of the interconnection charges levied by larger networks on their competitors. As additional services (such as broadband) became available, the regulatory solution of interconnection was extended as a blueprint to solve 'new' access problems, first in relation to local-loop unbundling and latterly in relation to access to other network elements.

163 Besides wholesale access in fixed networks, the EC started recommending national regulators to facilitate wholesale access in mobile networks in 2003.

164 Analysys Mason (2024), *The end of big capex: new strategic options for the telecoms industry*.

165 Asset lifetime varies somewhat across operators and markets; Ibid.

166 Ibid.

167 RCRWirelessNews (2023), *Spanish government aims to extend current spectrum licenses*.

Under the liberalisation process, regulators and policy makers have therefore had to contend with structural barriers to entry, related to the scale and cost of physical infrastructure needed to operate national networks, as well as decisions on the scope and modalities of market access, such as through licensing of and access to radio spectrum. These barriers to entry were compounded by the presence of historical monopolies at national level, whose incentives shifted to maximising profits and market share as they became for-profit, and in many cases private businesses. We consider each of these aspects in turn below, before going on to discuss the regulatory approach that has been taken to mitigate them later in this section.

Barriers to entry have arisen at all levels of the value chain, but are most pronounced at the infrastructure level, which has the greatest investment requirements, and relatively lower at the retail level, where regulation has facilitated market entry to the greatest extent.

Up-front cost of infrastructure

Deployment of infrastructure has arguably presented the most significant barrier to entry as the extensive physical networks required for the provision of telecoms services are costly to build. In the decades prior to liberalisation, incumbent operators built vast networks at significant cost (see Figure A.1) – often with state funding. This meant at the point of liberalisation, when fixed penetration rates were 131% for fixed lines in the EU,[168] they already had existing access to a mature customer base

Figure A.1: Annual investment in telecoms prior to liberalisation in the EU [Source: Analysys Mason based on EIB, 1998]

	1986–88 (USD billion)	1989–91 (USD billion)	1992–94 (USD billion)	1995–97 (USD billion)
Fixed	39.4	48.4	46.2	35.3
Mobile	0.5	1.2	2.6	12.2
Total	**39.9**	**49.6**	**48.8**	**47.5**

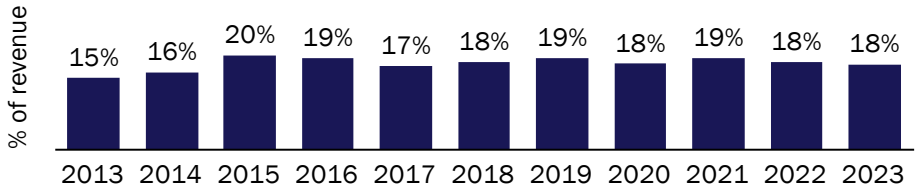
For new entrants, replicating this access was a key factor of success, but replicating the same infrastructure was economically unviable. Meanwhile, historical monopolies enjoyed the benefits of universal access throughout their respective countries, with large economies of scale and density, and network effects in telephony, which was the main consumer service offered over telecoms network prior to the introduction of DSL-based broadband. Highlighting this in its 1999 annual report, Telefónica noted that its post-liberalisation competitive advantage was "underpinned by its extensive, closely-knit network,… and its customers' loyalty".[169]

168 Penetration rate is over 100% as total fixed lines in the EU include residential and business lines, which were divided by residential households; see European Investment Bank, *Financing European Telecommunications: Facing The Challenges Of The Information Society*.

169 Telefónica (1999), Annual Report 1999, p.179.

Even once infrastructure is deployed, telecoms operators need to continue investing to maintain networks and adopt the latest technologies[170] resulting in stable capital intensity (see Figure A.2), which is also more challenging for new-entrant operators with a smaller customer base and hence lower revenue.

Figure A.2: Evolution of average capex intensity of the five largest telecoms operators in Europe,[171] 2013–23 [Source: Analysys Mason, operator reports]



Interconnection (later widened to include 'access') regulation was introduced to address these barriers, by forcing incumbent operators to provide wholesale access to their networks at regulated prices.

Economies of scale and network effects

In fixed networks (and most mobile networks too), large subscriber bases in densely populated areas result in lower average connection costs per user compared to smaller networks. These economies of scale and density improve margins and create further barriers for new entrants, which may find their smaller subscriber bases also geographically dispersed over wide areas. The large size of incumbents' subscriber bases also causes network effects, as discussed below.

Network effects in telephony reflect the fact that the utility of making a phone call depends on being able to reach the person one wants to call. This utility increases with the number of users, benefitting operators with greater market share. Although not as a legacy of former state ownership, the same dynamic has been important in mobile telephony, where incumbent operators have retained high market shares and large customer bases.

This meant that competitors would never be able to replicate the utility of the service provided by the incumbent without regulation of the modalities of interconnection to the incumbent's network for the purpose of interconnecting calls. As a result, interconnection regulation was introduced and remains a defining foundation of telecoms regulation to address the persistent structural issue of network effects.

170 Adoption of new technologies also requires up-front R&D costs (typically a capex expense), which in the telecoms industry is primarily handled by equipment vendors (e.g. Nokia and Ericsson) as discussed further in Section 3.2.1.

171 Operators were chosen based on highest subscriber numbers; the chosen operators are Deutsche Telekom, Orange, Vodafone, Telefónica and Iliad.

Licensing of electronic communications services and networks	The requirement for providers of telecoms services to be licensed is a barrier to entry that is addressed in the EU framework through the granting of general authorisations which allow service to be provided without the prior grant of a licence (although notification may be required). The EU framework seeks to further lower this barrier by constraining to a defined list of obligations that may be imposed at a national level in general authorisations.
Access to spectrum and numbers	Access to the scarce resources of spectrum and numbering also constitutes a structural barrier to entry in telecoms. The EU framework requires that the allocation of spectrum must be open, objective, transparent, non-discriminatory, based on proportionate criteria[172] and limits the conditions that may be imposed for spectrum use,[173] whilst rights to use numbering resources shall be granted through open, objective, transparent, non-discriminatory and proportionate procedures.[174] There is no clear parallel to this barrier to entry in the cloud sector.
Legacy of state ownership	Lastly, the fixed telecoms sector's history as state-owned monopolies left a legacy of direct benefits such as state-funded national infrastructure and very high (retail and wholesale) market shares in a mature market segment. Incumbent fixed and mobile operators are also generally vertically integrated, controlling everything from network infrastructure to retail service provision and customer relationships. The combination of vertical integration and the aforementioned network effects has created an incentive for these operators to refuse or obfuscate interconnection with new entrants in order to limit competition.[175]

To address historical monopolies in telecoms markets and support their transition to competition, regulations have been imposed to facilitate the new market entry and to create a level playing field, ensuring fair access to network resources from incumbents and promoting retail competition.

The requirements to fully liberalise telecoms by 1998[176] required Member States to remove all "special and exclusive rights" in key segments of the telecoms market including terminal equipment, satellite communications, cable TV and mobile communications. This was subsequently extended to telephony by the 1996 Full Competition Directive, which also set out the first European rules for licensing of operators, interconnection, numbering, directory services and universal services.

172 Article 48, EECC.

173 Article 49 EECC.

174 Article 94, EECC.

175 The asymmetry in network size created a 'termination monopoly', where the incumbent controlled access to a large portion of end users. New entrants needed to interconnect with the incumbent's network to reach these customers, giving the incumbent leverage to demand higher interconnection fees or impose other restrictive conditions.

176 Commission Directive of 28 June 1990 on Competition in the markets for Telecommunications Services (90/EC/EEC) as amended.

The preamble to this directive sets out the purpose of the introduction of the (at that stage novel) remedy of interconnection:

> *"(13) Subject to reasonable compensation, the right of new providers of voice telephony to interconnect their service for call completion purposes with the existing public telecommunications network at the necessary interconnection points, including access to customer databases necessary for the provision of directory information, is of crucial importance in the initial period after the abolition of the special and exclusive rights regarding voice telephony and telecommunications infrastructure provision. Inter-connection should in principle be a matter for negotiation between the parties, subject to the application of the competition rules addressed to undertakings. Given the imbalance in negotiating power of new entrants compared with the telecommunications organizations whose monopoly posi-tion results from their special and exclusive rights, it is likely that, as long as a harmonized regulatory framework has not been established by the Euro- pean Parliament and the Council, interconnection would be delayed by disputes as to terms and conditions to be applied. Such delays would jeopar-dize the market entry of new entrants and hence prevent the abolition of special and exclusive rights to become effective. The failure by Member States to adopt the necessary safeguards to prevent such a situation would lead to a continuation de facto of the current special and exclusive rights, which as set out above are considered to be incompatible with Article 90 (1) of the Treaty, in conjunction with Articles 59 and 86 of the Treaty.*
>
> *[...]"*

It goes on to explain the purpose of the original dispute resolution provisions in the European telecoms framework:

> *(14)*
>
> *[...]*
>
> *The absence of a quick, cheap and effective proce-dure to solve interconnection disputes, and one which would prevent the telecommunications orga-nizations causing delays or using their financial resources to increase the cost of available remedies under applicable national law or Community law, would make it possible for the telecommunications organizations to maintain their dominant position. Member States should therefore establish a specific recourse procedure for interconnection disputes."*

In parallel with liberalisation enabled by the Full Competition and Services Directive, the first harmonised European regulation was imposed by the various Open Network Provision (or ONP Directives).

Whilst the 1998 package of liberalisation and harmonisation directives started the development of a liberalised European telecoms sector, there were still significant national differences, so in 2002 these were replaced by the first fully harmonised framework comprising the Framework Directive

(2002/21/EC) and specific directives such as the Authorisation Directive (2002/20/EC), the Access Directive (2002/19/EC), and the Universal Service Directive (2002/22/EC). The 2002 package's overall aim was to provide 'a more harmonised and less onerous market access regulation for electronic communications networks and services throughout the Community'. One of its features was to allow for certain obligations, previously imposed in order to ensure the achievement of free competition, to be relaxed where the existence of competition could be established.

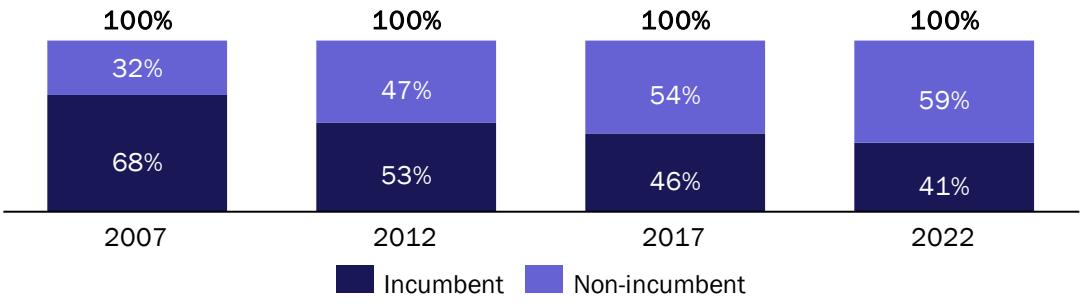
The 2002 directives were substantially amended and supplemented until in 2018 they were replaced by the EECC - Directive (EU) 2018/1972. Amongst its provisions are those relating to wholesale access, licensing, spectrum access and interconnection (including dispute resolution), which are summarised in 0 with accompanying purpose articulated in the EECC preamble:

Wholesale access regulation addressed barriers to entry, in particular those relating to up-front investment by allowing new entrant to provide services over the network of designated operators

Wholesale access and infrastructure re-use obligations have played a significant role in reducing barriers to entry in the fixed telecoms sector in particular. These regulatory measures mandated that incumbent (or those with market power) telecoms operators provide access to their existing networks and infrastructure to new entrants, often at regulated prices. This policy was designed (EECC Recital 155) to promote competition and ensure that end users benefit from a variety of services and providers. These obligations address market failures and ensure that essential facilities are available to competitors. They foster competition by allowing new competitors to enter markets and offer services without the prohibitive costs of building entirely new networks of sufficient scale from scratch.

By virtue of being granted access to existing networks, new entrants could use the infrastructure of established operators to offer competitive retail services. This not only reduced the initial capital expenditure required for market entry but also accelerated the time to market for new players. The regulatory approach therefore ensured that new entrants could begin operations sooner, with significantly lower up-front investment, making the market more dynamic and competitive and resulting in growth of non-incumbent market shares from nothing to over half of the retail market by 2017 (see Figure A.3).

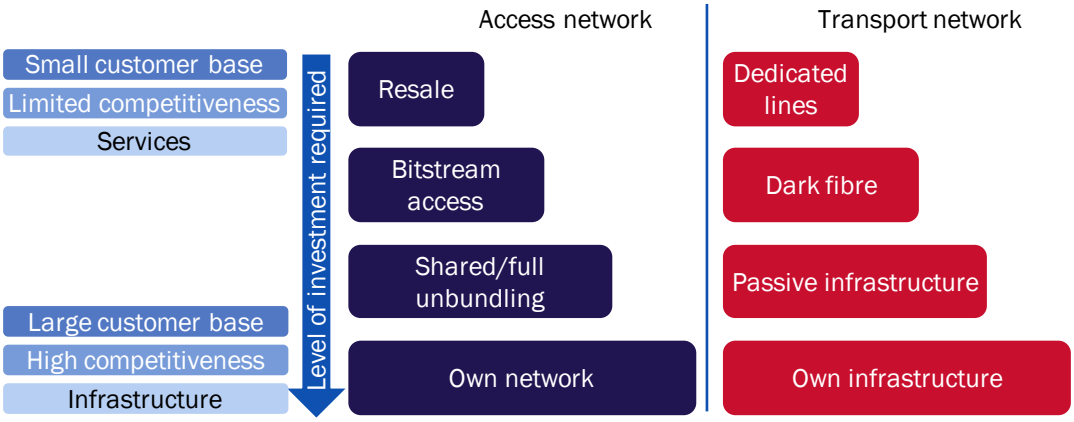
Figure A.3: Average fixed market share of connections (voice and broadband services) of EU incumbents versus non-incumbents [Source: Analysys Mason, 2024]



Initially, the primary goal of wholesale access was to enhance service-based competition. New entrants, often referred to as 'service providers', could lease network elements from incumbents at regulated wholesale rates.[177] This enabled them to offer differentiated services and competitive pricing to consumers, fostering a more vibrant market landscape. For instance, alternative operators like Digi Spain[178] and Sky Ireland[179] were able to rapidly scale their service offerings, by using incumbent networks, leading to improved service quality and reduced prices for consumers.

While service competition was the immediate focus, the long-term regulatory objective was to encourage new entrants to invest progressively in their own network infrastructure. This strategic approach, known as the 'ladder of investment', aimed to transition the market towards sustainable infrastructure-based competition. New entrants would start by using the broadest wholesale access services (e.g. where the role of the entrant was more or less limited to the retailing function) and gradually invest in their own network elements, such as switches, transmission systems, and eventually, local loops (see Figure A.4). This incremental investment strategy was designed to lower financial risk and build technical and operational expertise over time.

Figure A.4: Ladder of investment [Source: Analysys Mason, 2024]



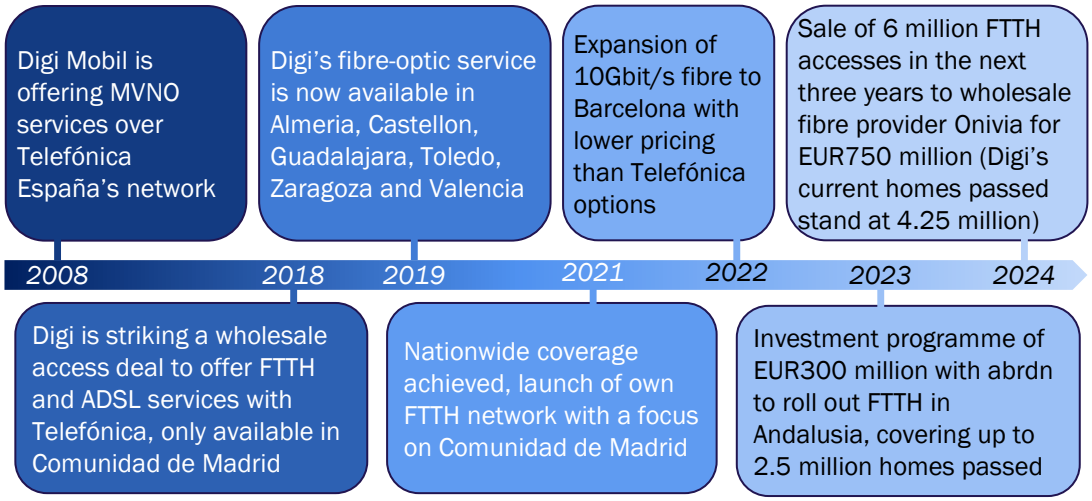
The pricing and terms of wholesale access were carefully set by regulators to balance the interests of incumbents and new entrants. Regulators set wholesale prices at levels that were low enough for new entrants to enter the market (i.e. for a new entrant to recover its cost of capital when operating on an 'equally efficient' or 'reasonably efficient' basis) but also incentivised them to eventually invest in their own infrastructure.

177 Cave, Martin (2006), *Encouraging infrastructure competition via the ladder of investment, Telecommunications Policy*, Vol. 30 (3–4), pp. 223–237.

178 Telecoms.com (2023), *Digi gets investment for €300 million Spain FTTH network*.

179 Sky (2023), *Sky Ireland and Virgin Media Ireland Announce Landmark Wholesale Deal*.

Figure A.5: Example of Digi Spain's path on the ladder of investment [Source:TeleGeography, press reports, Analysys Mason, 2024]



Digi in Spain, as shown in Figure A.5, demonstrates the evolution of this ladder of investment in recent years as it began offering services through a wholesale agreement on Telefónica's network in a limited geography, before expanding its geographical reach and eventually building its own fixed network in selected geographical areas.

Licensing and spectrum allocation regulation were revised to support new entrants through general authorisations and competitive awards for spectrum

As described previously, the requirement to obtain a licence to provide services and/or access to spectrum constitutes a structural barrier to entry. Whilst general authorisations mitigate the licensing aspect, access to spectrum has remained a challenge for new entrants in particular in the mobile market.

Whilst early spectrum bands for public mobile communications were assigned to incumbents prior to liberalisation[180] from the year 2000, and the introduction of third generation (3G), licences have been assigned through more competitive market-driven award process including beauty contests and more frequently (particularly in recent years) auctions. This, along with standardisation and co-ordinated timing of assignment (at least within individual Member States, and to an extent across different Member States), has given new entrants a chance to compete for access to spectrum.

Whilst giving new entrants an opportunity to compete for spectrum licences, these auction processes have often, nonetheless, posed challenges for them. Auctions were intended to promote efficient assignment of spectrum, with the potential competition benefits of allowing non-incumbents to compete for spectrum. In practice, they have often favoured incumbents with substantial financial resources and

180 GSMA (2015), *Spectrum for new entrants, lessons learned*.

established market positions, although in the early days of European auctions, there were often new-entrant friendly provisions (e.g. spectrum reservations) to try to mitigate these issues.

In summary, access to scarce resources such as spectrum was an issue that prevented competition from new entrants arising because it was just licensed to incumbents. However, policy has evolved to allow new entrants to fairly compete for access to spectrum. Where spectrum access remains a significant entry barrier, regulation has in some cases had to go further to try and mitigate these barriers to entry, which results in a complex and imperfect system. In the EECC, **article 48** requires that the procedures for the award of spectrum must be open, objective, transparent, non-discriminatory and proportionate.

Interconnection regulations addressed the benefits larger operators derived from network effects, preventing exclusionary practices such as refusal to interconnect and excessive pricing

As can be seen from the recitals to the Full Competition Directive, interconnection regulation was introduced at the same time as the withdrawal of incumbents' special and exclusive rights to provide voice telephony to enable new entrants to enter the market and provide end-to-end services. It was needed to ensure that the network effects associated with the integration of networks and services (primarily voice telephony, and subsequently SMS) were available across multiple network operators. This was also critical to enabling new entrants to be able to compete with established operators: a new entrant offering telephony services without being able to offer calls to existing operators' customers would have nothing to sell.

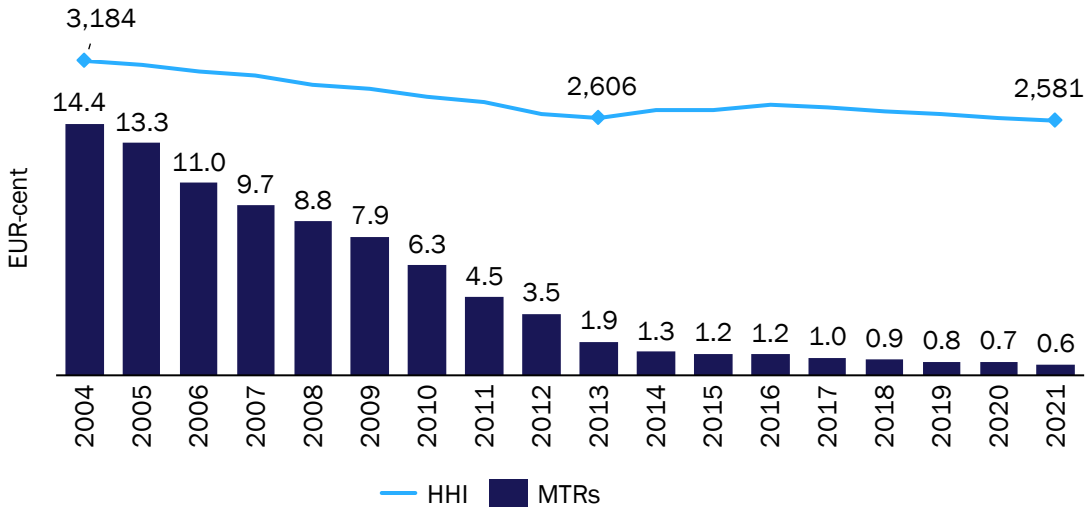
Outright refusal to interconnect has been a tactic to prevent or constrain competitors since the beginning of telecommunications as a mass market proposition.[181] Regulatory obligations to interconnect reduce this problem, but incumbents could and did exploit the asymmetry in network effects between a large established operator and a smaller new entrant though the imposition of excessive prices, in the form of voice and SMS termination rates way above (long-run) costs.

The regulation of interconnection conditions, and prices in particular, took nearly two decades. The 2002 regulatory regime imposed on NRAs the definition and analysis of 'call termination markets' that were systematically found to be non-competitive and required ex-ante regulation. This led to a progressive decline in regulated termination rates, and ultimately to a 2021 directive imposing a common price cap throughout the EU.[182]

181 See for example Tim Wu (2007), *A Brief History of American Telecommunications Regulation*.

182 European Commission, *COMMISSION DELEGATED REGULATION (EU) 2021/654 of 18 December 2020 supplementing Directive (EU) 2018/1972 of the European Parliament and of the Council by setting a single maximum Union-wide mobile voice termination rate and a single maximum Union-wide fixed voice termination rate* (Brussels, 2020, 2021/654).

Figure A.6: Average mobile termination rates (MTRs) and Herfindahl-Hirschman Index (HHI): time series of weighted average at European level [Source: BEREC, GSMA, Analysys Mason, 2021] [183]



The sustained reduction acted to lower the barriers to interconnection for smaller operators, which, given their size, were more likely to be connecting out to a larger operator and paying fees, than receiving incoming traffic and fees. The effects of this can be seen in Figure A.6, which demonstrates a correlation between reducing termination costs (in this case in the mobile market) and the reduction in the average competitive strength of incumbents.

A.3 Current European regulation recognises the progress made towards more effective competition and constrains the application of ex-ante rules to limited circumstances

Following their introduction, the regulatory measures outlined above have improved competition in the European telecoms sector and reduced reliance on incumbent infrastructure by incentivising challengers to invest in competing infrastructure over time.

The European telecoms sector is now primarily ex-ante regulated through the EECC. Recognising the increasing competition since the liberalisation of the European telecoms sector, the EECC imposes fewer onerous restrictions than earlier frameworks, minimising the application of ex-ante regulation. Nonetheless, it still addresses, and it is expected to continue to be needed, in order to continue to address, the key barriers to entry and persistent structural issues in the telecoms sector described in Annex A.2 above, as well as imposing telecoms-specific obligations such as ensuring consumer access to emergency services and number portability.

The EECC permits NRAs to impose and enforce defined ex-ante regulations under specific conditions to prevent anti-competitive practices which are not adequately addressed by ex-post

183 The HHI is a measure of concentration, from 0 to 10 000. The higher the HHI, the more concentrated the market. Here we calculated the weighted average based on each country's average rate and the share of subscribers for each country vs. all countries. Cyprus, Czechia, Slovenia and Turkey have been excluded in the HHI weighting due to data unavailability.

competition law. However, remedies are recognised as intrusive and are therefore tightly controlled to avoid unnecessary intervention and ensure proportionality. For example:

- **Article 61** describes the powers and responsibilities of the NRAs with regard to access and interconnection, limiting their ability to impose regulation only where "justified" or "to the extent necessary". It further guides NRAs to consider, among other areas, "the overriding need to support the incentive of the host to roll out the infrastructure in the first place". It mandates obligations imposed to be "objective, transparent, proportionate and non-discriminatory" and follow ongoing market developments through testing in renewed market analysis no later than five years after their application and withdrawn if market conditions no longer support them.

- **Articles 67** limits ex-ante regulation to relevant markets that pass a 'three-criteria test'[184] and to ensure any regulatory intervention is justified by a finding of SMP. If no SMP can be found, no ex-ante remedies can be applied.

- **Article 68** mandates NRAs to impose the "least intrusive way of addressing the problems identified" and reassess obligations in light of new market developments influencing competitive dynamics.

- The scope of ex-ante rules is further constrained by **Article 59**, which limits restrictions that hinder operators from negotiating agreements between themselves for access or interconnection.

Remedies available to NRAs range from obligations of transparency, non-discrimination and accounting separation to more intrusive remedies including obligations to provide access to civil engineering or network elements on regulated terms, price control or in exceptional cases, enforced functional separation of the wholesale business of the SMP entity.

NRAs can implement additional rules tailored to national market conditions, provided these rules are justified by thorough market analyses and align with the overarching objectives of the EU. These measures must be notified to the EC and other NRAs to ensure compliance with EU law. NRAs consult with the EC and BEREC to ensure a harmonised approach. This harmonisation process plays a crucial role to ensure that the measures do not raise serious doubts about their compatibility with EU regulations and general principles of EU law, including proportionality. Decisions may be appealed to the European Courts to the extent that they are incompatible with EU law.

Additionally, sector-specific regulation in the EU is complemented by ex-post EU competition law, which:

- prohibits anti-competitive behaviour: anti-competitive agreements and practices (article 101 TFEU), abuse of a dominant position (article 102 TFEU);

184 The three criteria are: "high and non-transitory structural, legal or regulatory barriers to entry are present", "there is a market structure which does not tend towards effective competition within the relevant time horizon, having regard to the state of infrastructure-based competition and other sources of competition behind the barriers to entry;" and "competition law alone is insufficient to adequately address the identified market failure(s)." See Article 67(1) EECC.

- reviews transactions which may have the effect of significantly impede effective competition in the EU (or a substantial part of it) (Merger Regulation).[185]

The EC takes primary responsibility for investigation and enforcement of competition issues in the EU[186] ,subject to appeal to the European Courts.

Competition cases in the telecoms sector reflect the economic characteristics described in Annex A.2 above: the behavioural cases are mainly concerned with abuse of dominant position (refusal to provide access,[187] exploitative or exclusionary pricing (i.e. margin squeeze[188]) with significant reviews of proposed transactions that seek to reduce the number of mobile competitors in the market.

In addition to the general competition rules, in 1997 the EC's competition section in 1997 issued a "Notice on the application of the competition rules to access agreements in the telecommunications sector - framework, relevant markets and principles." (**Access Notice**).

This dual approach provides a comprehensive framework to maintain market competition through both telecoms sector specific ex-ante regulation and general *ex post* competition law.

In accordance with the principle of proportionality, more intrusive ex-ante sector-specific regulation has only been maintained to the extent that competition law is unable to address issues: see in particular article 67(1) of the EECC, which expressly requires that an NRA must be satisfied that "*competition law alone is insufficient to adequately address the identified market failure(s)"* before sector-specific SMP regulation may be imposed.

However, because barriers to entry and persistent structural issues including network effects and economies of scale, scope and density at local levels are likely to continue to limit the effectiveness of competition in some areas, most notably wholesale access and interconnection[189] Telecoms-specific regulation is likely to persist.

185 Merger control requirements are reinforced for designated gatekeepers by the Digital Markets Act.

186 National competition authorities have the ability to address competition law compliance at a national level in instances where there is not a substantial effect on the wider EU.

187 Slovak Telekom a.s. contra Protimonopolný úrad Slovenskej republiky C-857/19.

188 Deutsche Telekom AG v European Commission C-152/19.

189 European Commission, *COMMISSION RECOMMENDATION on relevant product and service markets within the electronic communications sector susceptible to* ex-ante *regulation in accordance with Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code* (Brussels, 2020, SWD(2020) 143 final).

Annex B References to legal instruments and case law

B.1 Provisions in the EECC related to access to barriers to entry

Market analysis

Provisions

Article 67: This article requires NRAs to conduct regular market analyses to determine whether regulatory obligations are justified. NRAs must identify undertakings with significant market power (SMP) and impose appropriate obligations to ensure effective competition. Before imposing obligations, NRAs must:

- Define relevant markets in accordance with the Commission's guidelines.
- Analyse the defined markets to assess the level of competition.
- Identify undertakings with SMP based on the market analysis.
- Consult with stakeholders and the Commission on the proposed measures.
- Ensure that any imposed obligations are proportionate, justified, and based on the nature of the problem identified.

In particular, Article 67(1) states that:

> *"A market may be considered to justify the imposition of regulatory obligations set out in this Directive if all of the following criteria are met:*
>
> > *(a) high and non-transitory structural, legal or regulatory barriers to entry are present;*
> >
> > *(b) there is a market structure which does not tend towards effective competition within the relevant time horizon, having regard to the state of infrastructure-based competition and other sources of competition behind the barriers to entry;*
> >
> > *(c) competition law alone is insufficient to adequately address the identified market failure(s)."*

Article 74: This article allows NRAs to impose access obligations on undertakings with SMP to ensure effective competition in the market.

Reasons for Provisions (Recitals)

Recital 155: The purpose of access obligations is to promote competition and ensure that end users benefit from a variety of services and providers. These obligations address market failures and ensure that essential facilities are available to competitors.

Recital 156: Access obligations are necessary to address specific market conditions and ensure that services are available to all end users, particularly in areas where competition is limited.

Recital 157: Regular market analyses are essential to identify market power and impose appropriate regulatory obligations. This ensures that competition remains effective and that market conditions are continually assessed.

Licensing

Provisions

Article 12: This article requires providers to notify the NRA before commencing activities. The notification must include the provider's name, legal status, registration number, address, website, contact details, description of services, Member States concerned, and start date.

Article 13: This article sets out the conditions for general authorisation, including compliance with administrative charges, personal data protection, legal interception, public warnings, access obligations, and transparency obligations.

Article 48: This article outlines the procedures for granting rights of use for radio spectrum and numbering resources. The procedures must be open, objective, transparent, non-discriminatory, and proportionate.

Reasons for Provisions (Recitals)

Recital 40: Simplifying the regulatory environment by reducing administrative burdens encourages new market entrants and fosters innovation. This approach ensures that licensing conditions are proportionate and non-discriminatory.

Recital 41: Licensing conditions must be designed to promote competition and innovation while ensuring that providers comply with essential regulatory requirements.

Access to spectrum

Provisions

Article 48: This article specifies the application and selection procedures for granting rights of use for radio spectrum. The procedures must be open, objective, transparent, non-discriminatory, and proportionate. This ensures that new entrants have a fair opportunity to obtain spectrum rights.

Article 49: This article sets out the conditions for the use of radio spectrum, including the requirement for effective and efficient use and compliance with technical and operational conditions to avoid harmful interference. It also mandates the payment of fees for rights of use, which must be proportionate and non-discriminatory.

Article 51: This article provides for the transfer or lease of rights of use for radio spectrum. Providers must notify the NRA of their intention to transfer or lease rights and the effective transfer. The original conditions attached to the rights of use must be maintained, ensuring that new entrants can access spectrum through secondary markets.

Reasons for Provisions (Recitals)

Recital 114: Efficient use of radio spectrum is crucial for supporting wireless broadband coverage and the deployment of new technologies. Harmonized spectrum management ensures that spectrum resources are used effectively.

Recital 115: Shared use of radio spectrum maximizes efficiency and promotes innovation. This approach encourages the development of new services and technologies while ensuring that spectrum resources are used optimally.

Recital 116: Spectrum management should facilitate the entry of new market players and promote competition. This includes ensuring that spectrum is awarded in a way that supports competition at the end-user level.

Access to active and passive infrastructure

Provisions

Article 61: This article establishes the general framework for interconnection and access, ensuring that providers offer interconnection and access on fair and reasonable terms. It aims to promote competition and ensure that end users benefit from a variety of services.

Article 62: This article permits the imposition of obligations on undertakings with SMP to provide interconnection and access. These obligations ensure that other providers can interconnect and access essential facilities on fair and reasonable terms.

Article 70: This article permits the imposition of obligations non-discrimination obligations on undertakings with SMP to ensure that they provide equivalent conditions and quality of services to all providers.

Article 72: permits the imposition of obligations on undertakings to meet reasonable requests for access to, and use of, civil engineering including, but not limited to, buildings or entries to buildings, building cables, including wiring, antennae, towers and other supporting constructions, poles, masts, ducts, conduits, inspection chambers, manholes, and cabinets, in situations where, having considered the market analysis, the national regulatory authority concludes that denial of access or access given under unreasonable terms and conditions having a similar effect would hinder the emergence of a sustainable competitive market and would not be in the end user's interest

Article 73: This article permits the imposition of obligations on undertakings with SMP must meet reasonable requests for access to specific network elements and associated facilities. The conditions for such access must be fair, reasonable, and timely.

Article 74: This article allows NRAs to impose access obligations on undertakings with SMP to ensure effective competition in the market.

Reasons for Provisions (Recitals)

Recital 155: The purpose of access obligations is to promote competition and ensure that end users benefit from a variety of services and providers. These obligations address market failures and ensure that essential facilities are available to competitors.

Recital 156: Access obligations are necessary to address specific market conditions and ensure that services are available to all end users, particularly in areas where competition is limited.

Recital 157: Regular market analyses are essential to identify market power and impose appropriate regulatory obligations. This ensures that competition remains effective and that market conditions are continually assessed.

B.2 Provisions in the EECC related to barriers to switching

Barriers to switching

Provisions

Article 106: This article addresses barriers to switching by ensuring that end users can switch providers without undue obstacles. It mandates that switching processes be simple, quick, and free of charge. Providers must not impose contractual conditions or procedures that dissuade end users from switching.

Reasons for Provisions (Recitals)

Recital 274: The purpose of removing barriers to switching is to enhance consumer choice and promote competition. By making it easier for consumers to switch providers, the EECC aims to ensure that providers compete on the quality and price of their services, leading to better outcomes for consumers.

Recital 275: Simplifying the switching process reduces the risk of consumer lock-in and encourages providers to improve their offerings. This is particularly important in markets where consumers may be reluctant to switch due to perceived complexity or cost.

Enabling consumer switching

Provisions

Article 105: This article focuses on enabling consumer switching by ensuring that end users have access to clear and comprehensive information about their contracts and the switching process. Providers must offer facilities for consumers to monitor and control their usage, including timely information on consumption levels and alerts for abnormal consumption patterns. Additionally, providers must ensure that end users can terminate contracts without incurring further costs upon notice of changes in contractual conditions.

Reasons for Provisions (Recitals)

Recital 272: Enabling consumer switching is essential for promoting competition and ensuring that consumers can take advantage of better offers. By providing clear and comprehensive information, the EECC aims to empower consumers to make informed decisions about their service providers.

Recital 273: Access to usage information and alerts helps consumers manage their consumption and avoid unexpected charges. This transparency is crucial for building consumer trust and encouraging active participation in the market.

Number portability

Provisions

Article 106: This article also covers number portability, ensuring that end users can retain their telephone numbers independently of the service provider. Providers must complete the porting and activation process within one working day from the agreed date. Additionally, providers must ensure that the end user's service is not disrupted during the porting process.

Reasons for Provisions (Recitals)

Recital 276: Number portability is a key enabler of consumer switching, as it allows consumers to retain their telephone numbers when changing providers. This reduces the inconvenience and potential costs associated with switching, making it more attractive for consumers to seek better offers.

Recital 277: Ensuring that the porting process is quick and seamless minimizes service disruption and enhances consumer confidence in the switching process. This is particularly important for business users, who may rely on their telephone numbers for continuity of service.

B.3 Provisions in the EECC related to interconnection and access

Provisions

Article 61: This article establishes the general framework for interconnection and access. It mandates that providers offer interconnection and access on fair, reasonable, and non-discriminatory terms. The aim is to promote competition and ensure that end users benefit from a variety of services. Providers must negotiate in good faith and ensure that interconnection agreements are transparent and publicly available.

Article 62: This article imposes specific obligations on undertakings with significant market power (SMP) to provide interconnection and access. These obligations ensure that other providers can interconnect and access essential facilities on fair and reasonable terms. NRAs can impose obligations such as transparency, non-discrimination, accounting separation, access to specific network elements, and price control.

Article 27: This article outlines the dispute resolution mechanisms. It mandates that NRAs and BEREC play a key role in resolving disputes between providers. The aim is to ensure that disputes are resolved efficiently and effectively to maintain regulatory consistency. NRAs must resolve disputes within four months, and BEREC can provide opinions on cross-border disputes.

Reasons for Provisions (Recitals)

Recital 138: The purpose of interconnection and access obligations is to promote competition and ensure that end users benefit from a variety of services. By mandating fair, reasonable, and non-discriminatory terms, the EECC aims to create a level playing field where providers can compete effectively.

Recital 139: Effective dispute resolution mechanisms are crucial for addressing conflicts and ensuring regulatory consistency. NRAs and BEREC play a key role in resolving disputes and ensuring that regulatory decisions are implemented effectively. This helps maintain a stable and predictable regulatory environment, which is essential for fostering investment and innovation in the electronic communications sector.

Recital 140: Transparency in interconnection agreements is essential for ensuring that all market participants have access to the same information. This helps prevent anti-competitive practices and ensures that smaller providers and new entrants can compete on equal terms with established players.

B.4 Principles of EU law, electronic communications services, information society services and cloud services

Principle of equal treatment and non-discrimination

The principle of equal treatment requires that comparable situations must not be treated differently and different situations must not be treated in the same way, unless such treatment is justified on the basis of an objective and reasonable criterion and is proportionate to the aim pursued. This principle ensures fairness and prevents arbitrary discrimination in the application of laws and regulations.

Case law

Examples from EU case law have consistently upheld these principles. In Sky Österreich GmbH v Österreichischer Rundfunk, the Court held that any limitation on the freedom to conduct a business must be provided for by law, respect the essence of the right, and be proportionate to the legitimate aim pursued. In Finanzamt Köln-Altstadt v Roland Schumacker, the Court held that different treatment of non-residents compared to residents in tax matters must be justified by objective differences in their situations. In Spain v Commission, the Court emphasised that the principle of equal treatment is infringed if different situations are treated in the same way without objective justification.

Freedom to conduct a business

Article 16 of the Charter of Fundamental Rights of the European Union recognises the freedom to conduct a business, which includes the right to engage in economic or commercial activity, freedom of contract, and free competition. Limitations on this freedom are permissible under Article 52(1) of the Charter, but only if they are provided for by law, respect the essence of those rights and freedoms, and comply with the principle of proportionality. Such limitations must be necessary and genuinely meet objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others.

Case law

The freedom to conduct a business has been highlighted in several leading cases; in Sky Österreich GmbH v Österreichischer Rundfunk, the Court held that any limitation on the freedom to conduct a business must be provided for by law, respect the essence of the right, and be proportionate to the legitimate aim pursued. In Alemo-Herron and Others v Parkwood Leisure Ltd, it was emphasised that the freedom to conduct a business includes the right to contract freely and that any limitations must be justified and proportionate. In AGET Iraklis AE v Minister for Labour, Social Security and Social Solidarity, the Court ruled that restrictions on the freedom to conduct a business must be necessary and proportionate to the aim pursued, in this case, the protection of workers' rights.

Information society services (ISS)

ISS are defined across various EU directives and regulations as services normally provided for remuneration, at a distance, by electronic means, and at the individual request of a recipient of services. This definition is consistently referenced and applied in EU legislation, case law, and administrative decisions, emphasizing its broad applicability and importance in regulating digital services within the EU.

Legislation and statutes

The definition of ISS is primarily derived from Directive (EU) 2015/1535, which states that an ISS is "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services" (Directive (EU) 2015/1535). This definition is foundational and has been consistently referenced in subsequent EU regulations such as the Digital Services Act (Regulation (EU) 2022/2065) and the Digital Markets Act (Regulation (EU) 2022/1925), which both reaffirm the definition from Directive (EU) 2015/1535. Earlier, Directive 2000/31/EC also provided a broad description of ISS, including various online activities and explicitly excluding services like offline activities and broadcasting, which are not provided at the individual request of a recipient.

Case law

EU case law has consistently applied and interpreted the definition of ISS in line with the statutory provisions. Notable cases include Airbnb Ireland UC v Région de Bruxelles-Capitale, where the European Court of Justice classified an electronic platform's intermediation service as an ISS under Directive 2000/31/EC (Airbnb Ireland UC v Région de Bruxelles-Capitale). Similarly, in Asociación Profesional Elite Taxi v Uber Systems Spain, SL, the court held that an app-based transportation booking service met the criteria for an ISS. These cases underscore the application of the ISS definition to a variety of digital services, emphasising the role of electronic means and the individual request criterion.

Cloud services as information society services

Cloud services are classified as information society services under European Union law. This classification is supported by various legislative frameworks and judicial interpretations that define information society services as those normally provided for remuneration, at a distance, by electronic means, and at the individual request of a recipient of services. Cloud services, which offer computing resources and data storage over the internet, fit squarely within this definition.

Legislation and statutes

The European Union has consistently treated cloud services as a subset of information society services through various legislative acts. For instance, the Digital Services Act (Regulation (EU) 2022/2065) explicitly includes cloud computing within the scope of information society services by

defining them as intermediary services, which are a type of information society service ("This Regulation should apply to providers of certain information society services as defined in Directive (EU) 2015/1535...Examples of 'hosting services' include categories of services such as cloud computing"). Similarly, the NIS2 Directive (Directive (EU) 2022/2555) defines cloud computing services as digital services that enable on-demand administration and broad remote access to a scalable and elastic pool of shareable computing resources, aligning with the broader definition of information society services.

Moreover, the Data Act (Regulation (EU) 2023/2854) mentions cloud and edge services as part of data processing services, which are considered a subset of information society services, further supporting their classification under this category. The consistent inclusion of cloud services in these regulatory frameworks highlights their importance and relevance in the Digital Single Market of the EU.

Case law

Judicial interpretations have further solidified the classification of cloud services as information society services. Notable cases such as Asociación Profesional Elite Taxi v Uber Systems Spain, SL and VCAST Limited v RTI SpA have clarified the application of the definition of information society services to various online platforms, which by extension includes cloud services. For example, in Asociación Profesional Elite Taxi v Uber Systems Spain, SL, the court held that an intermediation service provided via a smartphone application meets the criteria for classification as an 'information society service' ("an intermediation service that enables the transfer, by means of a smartphone application, of information concerning the booking of a transport service...meets, in principle, the criteria for classification as an 'information society service'").

Examples of case law relevant to the definition of electronic communication services: SkypeOut and Gmail

The European Court of Justice considered the boundaries of what is an electronic communications service in two cases in 2019. In the first SkypeOut case, (Case C-142/18) the Court found that the SkypeOut service was an electronic communications service, whilst in the second Gmail case (C-193/18) the Court found that Gmail was not an electronic communications service.

In both cases, the Court referred back to the statutory definitions in the predecessor to the EECC and ruled that:

> a) The European regulatory framework makes a clear distinction between the production of content, which involves editorial responsibility, and transmission of content, which does not involve editorial responsibility.
>
> b) To fall within the definition of an electronic communications service, a service must involve the conveyance of signals, HOWEVER, whether the conveyance of signals is by means of an infrastructure that belongs to the service provider or not is not relevant to the

classification of the service – the question is whether the service provider is responsible vis-à-vis the end users for conveyance of the signal.

c) To be an electronic communications service, a service must consist '*wholly or mainly in the conveyance of signals on an electronic communications network*'.

In the SkypeOut case, the Court referred both to Skype taking end-to-end responsibility to its customers for the SkypeOut service, referencing Skype's interconnection agreements with other providers of electronic communications services for call termination, and that the SkypeOut service terminated on the PSTN as reasons to conclude that SkypeOut was an electronic communications service, notwithstanding Skype's arguments that it did not provide internet access or itself convey any signals.

In contrast, in the Gmail case whilst the court accepted that there was active participation of Google in the sending and receiving of emails, the Gmail could not be considered to be 'w*holly or mainly in the conveyance of signals on electronic communications networks*'.

B.5 Legal and regulatory frameworks applicable to cloud services

Cloud-related laws

General Data Protection Regulation (GDPR)	Reference: Regulation (EU) 2016/679 Key Obligations: • Data Protection Principles: Lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, and confidentiality. • Rights of Data Subjects: Right to access, rectification, erasure, restriction, data portability, and objection. • Data Security: Implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk. • Data Breach Notification: Obligation to report personal data breaches to the supervisory authority within 72 hours and communicate to affected individuals if high risk. • Data Processing Contracts: Controllers must ensure that processors provide sufficient guarantees to meet GDPR requirements.
Digital Markets Act	Reference: Regulation (EU) 2022/1925 Key Obligations: • Gatekeeper Identification: Certain large online platforms are designated as gatekeepers based on size and economic impact.

- Prohibited Practices: Prohibits gatekeepers from engaging in unfair practices, such as self-preferencing and restricting interoperability.
- Compliance Requirements: Gatekeepers must implement measures to ensure compliance, including reporting obligations and providing access to data for compliance monitoring.

Digital Services Act

Reference: Regulation (EU) 2022/2065

Key Obligations:

- Content Moderation: Platforms must implement mechanisms for content moderation, including notice-and-action procedures.
- Transparency Reporting: Regular reporting on content moderation activities, algorithmic decision-making, and advertising transparency.
- Risk Management: Very large online platforms (VLOPs) must assess and mitigate systemic risks, such as dissemination of illegal content and impacts on fundamental rights.

Digital Operational Resilience Act

Reference: Regulation (EU) 2022/2554

Key Obligations:

- ICT Risk Management: Financial entities must implement comprehensive ICT risk management frameworks.
- Incident Reporting: Obligations to report significant ICT-related incidents to competent authorities.
- Operational Resilience Testing: Regular testing of ICT systems to ensure operational resilience.

Data Governance Act (DGA)

Reference: Regulation (EU) 2022/868

Key Obligations:

- Data Intermediation Services: Establishes rules for providers of data intermediation services to ensure neutrality and trust.
- Data Altruism: Facilitates data sharing for the public good through recognized data altruism organizations.
- Public Sector Data: Encourages the re-use of certain categories of protected data held by public sector bodies.

Data Act

Reference: Proposal for a Regulation of the European Parliament and of the Council on harmonized rules on fair access to and use of data (2022)

Key Obligations:

	• Data Sharing Obligations: Facilitates access to and sharing of data generated by connected devices and related services. • Contractual Terms: Ensures fairness in business-to-business data sharing contracts. • Portability Rights: Enhances data portability for users to switch between cloud service providers.
Network and Information Security Directive (NIS Directive)	Reference: Directive (EU) 2016/1148 (NIS1) Key Obligations: • Security Measures: Operators of essential services and digital service providers must implement appropriate security measures. • Incident Reporting: Obligations to report significant incidents to national competent authorities. • National Frameworks: Member States must establish national NIS strategies and designate competent authorities.
Network and Information Security Directive 2 (NIS2 Directive)	Reference: Directive (EU) 2022/2555 Key Obligations: • Expanded Scope: Broader scope covering more sectors and types of entities, including medium and large entities. • Enhanced Security Requirements: Stricter cybersecurity risk management measures and reporting obligations. • Governance and Cooperation: Enhanced requirements for national authorities and stronger cooperation mechanisms among member states.
Platform-to-Business Regulation (P2BR)	Reference: Regulation (EU) 2019/1150 Key obligations: • Terms and Conditions (T&Cs): – Clarity and Accessibility: T&Cs must be written in plain and intelligible language and be easily accessible at all stages of the commercial relationship. – Grounds for Restriction: Platforms must clearly outline the grounds for decisions to restrict, suspend, or terminate services, and must provide a statement of reasons to the business user when such actions are taken. – Ranking Parameters: T&Cs must detail the main parameters determining the ranking of goods and services and the reasons for their importance.

  - Differentiated Treatment: Platforms must disclose any differentiated treatment given to their own products over those of business users, including the main economic, commercial, or legal considerations for such treatment.
  - Changes and Termination: Platforms must notify business users of any changes to T&Cs at least 15 days in advance, and provide information on how business users can terminate the contract if they disagree with the changes.

- Internal Complaint Handling: Platforms must establish an internal complaint-handling system, free of charge, to address business users' issues promptly, except for smaller businesses (less than 50 employees and €10 million turnover).

- Mediation: Platforms must identify at least two mediators in their T&Cs to resolve disputes that cannot be settled internally. These mediators must be based in the EU.

- Transparency Requirements: Platforms and search engines must disclose the parameters affecting search results and rankings, and if rankings are influenced by remuneration, they must describe the effects.

- Legal Enforcement: Business users and organizations with a legitimate interest can take legal action to ensure compliance with the P2B Regulation. Non-compliance can result in fines, and in some cases, imprisonment for corporate officers responsible for breaches.

Artificial Intelligence Act

Key obligations:

- Risk-Based Classification: AI systems are classified into categories based on their risk to health, safety, and fundamental rights: unacceptable risk, high risk, limited risk, and minimal risk.

- High-Risk AI Systems:

  - High-risk AI systems must meet strict requirements for data governance, documentation, transparency, human oversight, and robustness.
  - Providers of high-risk AI systems must register them in an EU database before they can be marketed.

- Transparency Obligations: AI systems interacting with humans, used for biometric identification, or generating deepfakes must inform users that they are interacting with an AI system.

- Compliance and Enforcement: National supervisory authorities will monitor and enforce compliance with the AI Act. Non-compliance can result in significant fines.
- Governance Framework: The Act establishes a European Artificial Intelligence Board to facilitate the implementation of the regulation and promote cooperation among member states.

General law (relevant selection)

EU Competition Law

Relevant Legislation: Articles 101 and 102 of the Treaty on the Functioning of the European Union (TFEU).

- Article 101 TFEU: Prohibits agreements between companies that restrict competition. This includes price-fixing, market sharing, and other collusive practices.
- Article 102 TFEU: Prohibits the abuse of a dominant market position. This includes practices such as predatory pricing, exclusive dealing, and refusal to supply essential facilities.

EU Merger Regulation:[190]

- Avoid Anti-Competitive Agreements: Cloud service providers must not engage in agreements or concerted practices that restrict competition. This includes not fixing prices, limiting production, or dividing markets.
- Prevent Abuse of Dominance: Dominant cloud service providers must not exploit their position in a way that harms competition. They must ensure fair pricing, provide access to essential facilities, and avoid exclusionary practices.
- Merger Control: Large mergers and acquisitions must be notified to the European Commission for approval. This is to ensure that such consolidations do not harm competition.

Unfair Commercial Practices Directive

Relevant Legislation: Directive 2005/29/EC

Key Obligations:

- Prohibition of Misleading Actions and Omissions: Cloud service providers must not provide false information or omit important facts that could mislead consumers.

190 Council Regulation (EC) No 139/2004 of 20 January 2004 on the control of concentrations between undertakings.

- Ban on Aggressive Practices: Providers must not use harassment, coercion, or undue influence to sell their services.

Consumer Rights Directive

Relevant Legislation: Directive 2011/83/EU

Key Obligations:

- Pre-Contractual Information: Providers must give clear information about the service, including its main characteristics, total price, duration, and conditions for terminating the contract.
- Right of Withdrawal: Consumers have the right to withdraw from contracts within 14 days without giving any reason.
- Delivery of Digital Content: Providers must deliver digital content promptly and ensure it is functional and meets the contract description.