cerre Centre on Regulation in Europe

COMPETITION AND REGULATION OF CLOUD COMPUTING SERVICES:

ECONOMIC ANALYSIS AND REVIEW OF EU POLICIES

REPORT
February 2024

Antonio Manganelli
Daniel Schnurr

As provided for in CERRE's bylaws and procedural rules from its "Transparency & Independence Policy", all CERRE research projects and reports are completed in accordance with the strictest academic independence.

The project, within the framework of which this report has been prepared, received the support and/or input of the following CERRE member organisations: Arcep, Amazon, ComReg, Microsoft, Vodafone. However, they bear no responsibility for the contents of this report. The views expressed in this CERRE report are attributable only to the authors in a personal capacity and not to any institution with which they are associated. In addition, they do not necessarily correspond either to those of CERRE, or of any sponsor or of members of CERRE.

TABLE OF CONTENTS

ABOUT CERRE

Providing top quality studies and dissemination activities, the Centre on Regulation in Europe (CERRE) promotes robust and consistent regulation in Europe's network and digital industries. CERRE's members are regulatory authorities and operators in those industries as well as universities.

CERRE's added value is based on:

- its original, multidisciplinary and cross-sector approach;
- the widely acknowledged academic credentials and policy experience of its team and associated staff members;
- its scientific independence and impartiality;
- the direct relevance and timeliness of its contributions to the policy and regulatory development process applicable to network industries and the markets for their services.

CERRE's activities include contributions to the development of norms, standards and policy recommendations related to the regulation of service providers, to the specification of market rules and to improvements in the management of infrastructure in a changing political, economic, technological, and social environment. CERRE's work also aims at clarifying the respective roles of market operators, governments and regulatory authorities, as well as at strengthening the expertise of the latter, since in many Member States, regulators are part of a relatively recent profession.

ABOUT THE AUTHORS

Antonio Manganelli is professor of Antitrust and Regulation at University of Rome LUMSA, where he is also programme coordinator for the M.Sc. in Antitrust, Regulation and Innovative industries. Antonio holds a Ph.D. in Law and Economics from the University of Siena.

He previously worked as Research Associate at the European University Institute and in a number of public institutions, i.e., the Italian Ministry of Economic Development as Deputy Head of Cabinet, the OECD as national expert, the Italian NRA for Telecom and Media (AGCOM), the UK Competition and Markets Authority (CMA), the Office of the Body of European Regulators for Electronic Communications (BEREC).

Daniel Schnurr is a CERRE Research Fellow and a Professor of Information Systems at the University of Regensburg, where he holds the Chair of Machine Learning and Uncertainty Quantification. Previously, he was head of the research group Data Policies at the University of Passau. He received his Ph.D. in Information Systems from the Karlsruhe Institute of Technology, where he previously studied Information Engineering and Management. Daniel Schnurr has published in leading journals in Information Systems and Economics. His current research focuses on the role of artificial intelligence for competition, privacy and data sharing in digital markets, as well as regulation of AI and the data economy.

EXECUTIVE SUMMARY

Cloud infrastructures and services have become key building blocks of the digital society. As more businesses and organizations migrate their infrastructure and services to the cloud, the cloud industry is rapidly growing and has by now become a key enabler of digital businesses and a vital infrastructure for the economy as a whole. At the same time, the digital technologies that enable cloud infrastructures and services are constantly evolving, thus facilitating the development of new cloud services, most notably in the areas of artificial intelligence and the Internet of Things.

Given its strategic and economic importance, the European Union (EU) and Member States are increasingly intervening in the cloud sector. When presenting the Political Guidelines of the incoming European Commission in 2019, President Ursula von der Leyen referenced the cloud as a cornerstone of a European digital infrastructure fit for the future. Following its European strategy for data, the Commission has proposed a myriad of policy initiatives on cloud computing. Several of these initiatives have recently been adopted as regulations, most notably the Data Act (DA) and Digital Markets Act (DMA), while other cloud initiatives and issues continue to be debated. At the same time, there are ongoing investigations on the national level into the cloud computing industry with a focus on competition issues and the proper functioning of these markets. Besides these policy interventions, there have been several stakeholder initiatives and self-regulation activities in the European cloud sector and related industries.

This CERRE research report takes stock of the recent developments and major policy updates in the EU with a focus on competition and the proper functioning of markets in the cloud computing industry. To this end, the report provides a coordinated legal review and analysis of the recent policy initiatives as well as an economic analysis of the competition issues that arise with regard to the peculiar economic and technical characteristics of cloud computing. In this vein, the report provides an economic and legal assessment of the recently adopted policies and regulations as well as their justifications from an economic perspective. Furthermore, the report contributes to the ongoing and future policy process by informing the interpretation and implementation of already adopted policies as well as decisions on further policies and interventions.

The legal assessment provides a cross-cutting analysis of all pieces of legislation involved in cloud regulation by selecting the relevant provisions for the policies that have a broader scope, most notably the DA and the DMA, as well as by attempting systemic interpretations of provisions enshrined in the different acts, yet, directly or indirectly, interplaying. The report highlights several areas where further clarification is required with respect to the adopted and proposed policies and their precise interpretation. Moreover, the analysis identifies several problems of coherence and consistency between different regulations. The economic assessment investigates competition issues that may arise from the specific characteristics of cloud computing services and analyses possible regulatory approaches to address competition concerns. To this end, the report analyses vendor lock-in and economies of scale and scope as potential sources of market inefficiencies and evaluates their impact on competition in the cloud computing industry. Based on this analysis the report highlights the economic trade-offs that arise in the context of different regulatory approaches and remedies that have been recently proposed or are currently discussed as policy options. In this vein, the economic

analysis is intended to inform the application of current cloud regulations such as the DA as well as to provide a guiding economic framework for other cloud initiatives on the EU level and ongoing investigations at the national level. Building on the legal and economic analysis, the report derives the following six overarching recommendations on current and future policies for cloud computing in the EU.

Recommendation 1: The legal interpretation within and across policies should be clarified by providing guidelines in order to address problems of coherence and cross-consistency as well as to reduce uncertain legal interaction effects, also by issuing the Cloud Rulebook.

EU legislation and policies about cloud services comprise several different pieces of legislation and actions, covering technological, economic, and legal aspects, and aiming at different kinds of results in terms of competition, competitiveness, and consumer protection (see Section 3). Coherence and cross-consistency of all regulations, ranging from a clear and consolidated definition of the main legal concepts involved to their respective scopes of application and their possible interplays, should be a primary objective both when conceiving the substantial rules and when drafting the legal documents. With respect to the current EU policy framework, this has been found particularly important for obligations concerning data portability, (vertical and/or horizontal) interoperability, and functional equivalence, primarily in the DA (see Section 3.2) yet also across other pieces of legislation when these concepts are adopted. To a certain extent, this problem could and should be tackled through the long-awaited Cloud Rulebook, which may play a crucial role in providing extensive clarifications, albeit non-legally binding, based on a systemic interpretation of all pieces of legislation involved in cloud regulation, as well as providing clarifications on whether and where the adopted voluntary self-regulatory codes are still playing a role in the cloud regulation.

Recommendation 2: As for the DMA enforcement, the Commission should thoroughly consider all specific features of cloud services vis à vis other core platform services, in particular, by applying the proportionality principle, both to the designation of gatekeepers and to the application of remedies, in order to avoid internal incoherence and regulatory anomalies.

The DMA is of pivotal importance for competition policy and consumer/business users' empowerment in digital markets. However, because of the many nuances and specificities of cloud services as core platform services, that is, primarily the overall lack of two-sidedness (except for marketplaces, see Section 4.2.2), it is extremely difficult to find a systemic interpretation of the basic concepts of end users, business users, and gatekeepers under the DMA (see Sections 3.3.2 and 3.3.3). In turn, this can make it very difficult to have a designation of cloud service gatekeepers that is at the same time both operational and meaningful under an economic regulation perspective. Moreover, only a subset of DMA obligations seems to be relevant and applicable in the context of cloud computing (see Section 3.3.4). To soften these pitfalls and to mitigate the risks of unintended consequences, the DMA should be interpreted and applied considering the proportionality principle, which is explicitly mentioned in the DMA at Recital 28 for emerging undertakings. According to the proportionality principle, each regulatory measure should be meaningful and necessary to reach the regulatory objective when the same result can't be achieved by putting in place a less intrusive action. Operationally, this should translate into considering all the basic concepts for gatekeepers' designation as well as for possible

rebuttal actions in a coordinated and consistent fashion, and, in case of designation, in imposing only a subset of obligations that are meaningful considering the market structure of a gatekeeper for cloud services.

Recommendation 3: Establish a clear institutional framework for the enforcement of the existing rules to avoid too much fragmentation.

The DMA and the DA are two distinct pieces of regulation, and this report has identified potential inconsistencies between the two, which may (or may not) produce enforcement problems. There is a risk that their parallel application could create uncertainty, and this risk is magnified by the differences in enforcement setting (see Section 3.4.2). Indeed, the strikingly asymmetric institutional design of the DA vis à vis the DMA could result in a problematic lack of coordination in the application of the two pieces of legislation. Moreover, fragmentation within the national enforcement level should be avoided. These problems could be addressed, inter alia, by: (i) maintaining a decentralised enforcement for the DA, yet establishing strong formal coordination mechanisms (as it is the case for telecom National Regulatory Authorities (NRAs), BEREC and EU Commission for example); and (ii) reducing national fragmentation by allocating new competences defined by the DA to already existing national authorities (as defined in previous EU legislation). This would not go against the principle that each Member State is competent to identify and designate national enforcers, as the EU rules would only identify bundles of competences (defined in different normative acts), in an abstract manner, which will be detailed by each member state; and (iii) the European Commission should exercise its discretion toward a clearer centralisation for EU competition law enforcement in digital markets and services regulated by the DMA, especially when gatekeepers are under investigation, in order to avoid legal uncertainties.

Recommendation 4: Regulatory interventions should consider the specific economic and technical characteristics of the cloud computing industry as well as the strategic decision-making of cloud customers. In general, there is evidence of competition among cloud providers, especially for customers who migrate to the cloud for the first time. However, competition concerns may arise from factors that facilitate vendor lock-in, particularly when markets are concentrated because of significant economies of scale and scope.

The review of European policy initiatives demonstrates that several of the recent policy interventions have been motivated, among other factors, by concerns about the proper functioning of markets in the cloud computing industry. In particular, the recently adopted DA aims to facilitate customer switching and multi-vendor cloud approaches by introducing a range of new cloud regulations (see Section 3.2). In our analysis of competition issues, we focus on whether vendor lock-in and economies of scale and scope give rise to market inefficiencies that could justify regulatory intervention from an economic perspective (see Section 4). In this vein, our analysis of the underlying economics of cloud computing can inform the assessment and implementation of the recently adopted provisions of the DA but also serve as a guiding framework for future cloud policy initiatives.

Economies of scale and scope represent key characteristics of cloud computing services. In particular, at the Infrastructure as a Service (IaaS) layer, economies of scale can facilitate concentration when not

offset by the benefits of specialisation (see Section 4.2.1). Nonetheless, there are indications of competition between providers of IaaS services in today's markets, even though a large share of the markets, including the take-up of new customers, is captured by large cloud service providers, known as hyperscalers. Compared to the IaaS layer, market entry at the PaaS layer and the SaaS layer is significantly easier, as application developers and service providers can make use of cloud infrastructure services themselves. In turn, this can raise concerns about a competitive level playing field when independent software vendors (ISVs) compete with the same hyperscalers that they also rely on with respect to access to IaaS services (see Section 4.2.2). Even if ISVs do not rely on competitors' IaaS services, integrated cloud providers frequently have a competitive advantage due to their ability to offer ecosystems with a broad range of services. However, these integrated ecosystems also offer benefits and efficiencies to customers due to economies of scope and benefits from the technical integration of cloud services. Overall, the cost and demand characteristics of cloud services give rise to a general welfare trade-off between efficiencies from large-scale operations and integrated ecosystems, on the one hand, and higher concentration among cloud service providers, on the other hand (see Section 4.2.3). Therefore, we suggest that the general focus of regulation and competition policy should be on (i) monitoring the ability of ISVs to enter and compete with respect to their specific services markets and (ii) safeguarding and promoting competition intensity by reducing switching costs to the extent this promotes the lock-in of customers. While the DA already aims to achieve these objectives, we make several observations on its legal implications in Section 3 and provide an in-depth analysis of the involved economic trade-offs for specific regulatory interventions in Section 5.

The possibility and extent of vendor lock-in in cloud computing are determined by the interplay of different types of switching costs and, ultimately, the sum of switching costs that accumulates for a customer (see Section 4.1). When assessing the competitive implications of switching costs, it is important to consider customers as strategic actors and the extent of their ability in specific markets to negotiate ex-ante benefits that can compensate for higher long-term prices due to the presence of switching costs. The ability and resources to negotiate such upfront benefits can vary among customers (see Section 4.1.4), depending, among other factors, on customer characteristics (such as the size of its operations) and their own business decisions (such as the choice for specific technologies and the commitment to longer term contracts).

In general, we consider that data-induced switching costs, technical incompatibility, and data egress fees can together constitute significant costs for switching and may give rise to vendor lock-in for certain types of customers and services (see Sections 4.1.1 to 4.1.3). These switching costs can result from both the strategies and actions of a cloud service provider as well as customers' demands and decisions. Whereas committed spend discounts can add to the switching costs of customers, these and similar practices (like cloud credits) are associated with direct (often short-term) benefits for customers and any regulatory intervention should therefore be treated with particular caution (see Section 4.1.4). With respect to interoperability, our analysis highlights that, in the context of vendor lock-in, interoperability may not be seen so much as an ultimate and universal end in itself, but as a potential means to decrease switching costs from technical incompatibility (see Section 4.1.2). In particular, by facilitating multi-cloud approaches, interoperability could provide customers with a

more credible threat of switching, thus improving their negotiation position vis-à-vis their current cloud provider.

Recommendation 5: Remedies to address competition concerns in cloud computing involve important and manifold economic trade-offs. In general, our analysis suggests that remedies, which directly limit the (often short-term) benefits of customers (such as interventions into committed spend discounts and cloud credits), should be treated with particular caution, whereas data portability regulation and cost-based regulation of data egress fees are better suited to address structural barriers to switching and multi-cloud approaches.

Based on our analysis of the economic trade-offs that arise from different regulatory approaches and remedies (see Section 5), we suggest that regulatory intervention should prioritise addressing structural barriers to switching and multi-cloud approaches. To minimise adverse effects from regulatory intervention, we argue that remedies should focus on empowering customers as strategic actors that internalise the central trade-off between short-term benefits and long-term costs of cloud service adoption and multi-cloud cloud approaches.

In this vein, we view data portability as a promising general approach to address technical barriers to switching providers (see Section 5.1). To limit implementation costs and complexity, we suggest that the default requirement for portable data should be to make data available to customers in a structured, commonly used, open and machine-readable format. Hence, we believe that the criteria imposed by Article 30 (5) of the DA represent a suitable default for data portability. In contrast, mandatory standardisation of data formats (as under Articles 30 (3) and 33 DA) should be limited to selected cases, where services are more clearly homogeneous to a certain degree, markets are concentrated, and data portability is of high value to customers.

Price regulation of charges from cloud providers for moving or transferring data from the cloud storage where it was initially uploaded to an external destination, known as data egress fees, can decrease financial switching costs and thus reduce the risk of vendor lock-in. This comes at the cost of limiting cloud providers' freedom to set prices and entails the risk of distorting price signals. Whereas price regulation can have pro-competitive effects by reducing potentially excessive prices, there is the risk that service providers will recoup the costs of external data transfers through increased prices for all cloud users (see Section 5.3). In line with the DA's provisions on data egress fees for the general operations of multi-cloud approaches (Art. 34 (2) DA), we consider cost-based price regulation a suitable approach to balancing this trade-off if financial switching costs are found to constitute a significant barrier for switching or for establishing multi-cloud approaches. We suggest that transit prices may serve as a market-driven benchmark and general proxy for cost-based regulation of egress fees. In contrast to the DA's provision on data egress fees for the purpose of switching (Art. 29 (1) DA), we generally advise against a zero-price regime for data egress fees. Whereas such an approach fully eliminates data-related financial switching costs for customers and therefore could benefit smaller providers through increased customer switching, it prohibits cloud service providers from directly recovering any of the costs for external data transfer, which creates socially inefficient incentives for providers and customers. Furthermore, if applied symmetrically as by the DA, a zero-price regulation

could pose a substantial business risk for smaller providers, as cross-subsidisation of data traffic costs is more difficult for these providers.

Finally, we highlight that interventions into the pricing practices of cloud providers with respect to limiting or prohibiting committed spend discounts and cloud credits (which have been the subject of investigations at the national level) involve risks of inadvertently constraining competition and thus lowering the (often short-term) benefits of competition made available to customers (see Section 5.4). This is particularly the case if other significant switching costs for customers persist. Hence, any (mostly long-term) benefits from intervening in such pricing practices in terms of lower switching costs or remedying anti-competitive effects should be carefully weighed against the general risks of limiting competition and hurting customers. In addition, there are particular innovation and efficiency benefits from committed spend discounts and cloud credits being available as pricing instruments for cloud providers. Non-discrimination obligations on these pricing practices may benefit existing customers at the expense of new customers, but the overall net benefit for customers is unclear and could likely be detrimental to overall competition.

Recommendation 6: Regulatory efforts to promote interoperability for multi-cloud approaches should aim to facilitate and safeguard the development of market-driven interoperability solutions that can bridge heterogeneities between providers' services. Mandatory regulated standards should be considered as a last resort, as expected benefits must be significant to exceed the general negative effects and challenges of enforced standardisation.

Although often referred to as a global concept for cloud computing, the benefits and costs of interoperability regulation must be assessed with reference to specific cloud services and use cases. Mandatory standards (as envisioned by Art. 33 DA) are the most effective way to establish interoperability but can entail negative effects on cloud providers' flexibility and freedom to differentiate their services (see Section 5.5.1). This can reduce service variety and impede innovation. As an alternative, regulation may aim to promote market-driven and custom-made interoperability solutions that can bridge heterogeneities between providers' services (see Section 5.5.2). To this end, regulation may require cloud service providers to make APIs and accompanying documentation available for specific services. In addition, regulation may impose safeguards against abrupt changes and termination of interfaces with the exception of explicit and specific threats to the security or integrity of cloud services. These restrictions on cloud providers' freedom have similar but likely less significant negative effects than mandatory standards, as they preserve more flexibility and freedom for cloud providers and their service offerings.

1. INTRODUCTION

Cloud infrastructures and services have become key building blocks of the digital society. As more businesses and organisations migrate their infrastructure and services to the cloud, the cloud industry is rapidly growing and has become a key enabler of digital businesses and a vital infrastructure of the economy as a whole. This dynamic is accompanied by the constant evolution and progress of digital technologies that enable cloud infrastructures and services as well as the emergence of new cloud services, especially in the context of artificial intelligence and the Internet of Things.

Given its strategic and economic importance, the European Union (EU) and Member States are increasingly intervening in the cloud sector. When presenting the Political Guidelines of the incoming European Commission in 2019, the newly elected President Ursula von der Leyen referenced the cloud as a cornerstone of a European digital "infrastructure fit for the future".[1] In its European strategy for data, the Commission further stressed that the "digital transformation of the EU economy depends on the availability and uptake of secure, energy-efficient, affordable and high-quality data processing capacities, such as those offered by cloud infrastructures and services […]".[2] Following the data strategy and the Commission's guidelines, the current Commission has recently enacted a myriad of policy initiatives and regulations that have been concerned with competition in the cloud industry, interoperability issues, cloud security and the flow of data, industrial policy for the cloud sector, as well as financial support for cloud R&D and deployment.[3]

With the Digital Markets Act and the Data Act, the European Union has adopted two landmark regulations that, among other areas, address competition and interoperability issues in the cloud sector. With these regulations, the EU imposes new obligations for digital gatekeepers as well as new horizontal rules that will apply to all cloud service providers in the EU. Most prominently, the regulations introduce new rules that are intended to improve the portability of customers' data, facilitate the switching of customers between different cloud service providers, and introduce new measures aimed at promoting interoperability of cloud services.[4]

At the same time, competition authorities at the national level have been undertaking investigations into the cloud markets with a focus on the well-functioning of these markets. Both, in the Netherlands and France, the respective competition authorities have released market studies on the cloud sector

[1] Von der Leyen (2019). Speech in the European Parliament Plenary Session 27 November 2019, p. 42. https://op.europa.eu/en/publication-detail/-/publication/62e534f4-62c1-11ea-b735-01aa75ed71a1

[2] European Commission (2020). A European strategy for data. COM(2020) 66 final, p. 9.

[3] Regulation on contestable and fair markets in the digital sector (Digital Markets Act) [2022] OJ L 265/1; European Commission (2022). Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access and use of data (Data Act). COM(2022) 68 final; Directive on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). [2022] OJ L 333/80. ENISA (2020). Cloud Certification Scheme: Building Trusted Cloud Services Across Europe. https://www.enisa.europa.eu/news/enisa-news/cloud-certification-scheme. European Commission (2023). European Alliance for Industrial Data, Edge and Cloud. https://digital-strategy.ec.europa.eu/en/policies/cloud-alliance. European Commission (2023). The Digital Europe Programme. https://digital-strategy.ec.europa.eu/en/activities/digital-programme

[4] European Commission (2023). Data Act: Commission welcomes political agreement on rules for a fair and innovative data economy. https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3491

that identify potential risks to competition.[5] In April 2023, Ofcom released the intermediary findings of its market study into cloud infrastructure services in the UK, identifying several competition concerns and considering a referral to the Competition and Markets Authority (CMA) to carry out a follow-up market investigation.[6]

Besides these policy interventions, there have been several industry-led initiatives and self-regulation activities in the European cloud sector and related industries. For example, the multi-stakeholder association 'Switching Cloud Providers and Porting Data' (SWIPO) has been established to develop codes of conduct for cloud providers as foreseen by the EU Free Flow of Non-Personal Data Regulation.[7] Furthermore, the Gaia-X initiative aims to establish a federated system linking different cloud providers together under a common governance framework promoting "transparency, controllability, portability and interoperability across data and service".[8]

This CERRE research report provides an overview and assessment of these recent policy initiatives and legislations in the European Union with a particular focus on potential competition issues. To this end, the report reviews the recent policy initiatives and analyses the coherence and consistency of these initiatives from a legal perspective. Furthermore, the report provides an economic analysis of potential market failures that could justify regulatory interventions in the cloud sector. Based on this analysis, the report highlights the economic trade-offs that arise in the context of different remedies that have been recently proposed or are currently discussed. Building on the legal and economic analysis, the report derives recommendations on current and future policies for cloud computing in the EU.

The report integrates a broad review of recent policy initiatives but focuses on competition issues in its analysis. In this context, it is important to note that cloud policies are influenced by a broad range of motives and policy goals (for instance, national security or industrial policy goals), which may add additional perspectives and arguments on the issues that are discussed in the report. It is however beyond the scope of this report to provide an exhaustive analysis of all policy perspectives (such as sustainability and cyber security). Nonetheless, the economic well-functioning of the cloud computing industry will be of major importance for all these policies and their respective goals, which is why we consider the issues analysed in this report to be central for any broader policy framework on cloud computing.

The remainder of this report is organised as follows. Section 2 gives a brief overview of the key characteristics of cloud computing services and the current state of the European Cloud Computing industry. Section 3 reviews recent policy initiatives on cloud computing at the EU level with a particular focus on the Data Act and the Digital Markets Act. In addition, current market investigations at the national level are summarised. Section 4 analyses the specific characteristics and issues of the cloud computing industry from an economic perspective and evaluates their impact on effective competition

[5] Authority for Consumers and Markets [ACM] (2022). Market study into cloud services. https://www.acm.nl/system/files/documents/public-market-study-cloud-services.pdf. Autorité de la concurrence (2023). Summary of Opinion 23-A-08 of 29 June 2023 on competition in the cloud sector. https://www.autoritedelaconcurrence.fr/sites/default/files/2023-06/Resume_Avis_Cloud%20EN_final_2023_2906.pdf

[6] Ofcom (2023). Cloud services market study. Interim report. https://www.ofcom.org.uk/__data/assets/pdf_file/0029/256457/cloud-services-market-study-interim-report.pdf

[7] Regulation on a framework for the free flow of non-personal data in the European Union. [2018] OJ L 303/59.

[8] Gaia-X (2023). What we are. https://gaia-x.eu

in cloud computing. In particular, the section focuses on whether vendor lock-in and economies of scale and scope give rise to market failures. Section 5 considers various regulatory approaches and remedies to address competition issues in cloud computing and highlights the manifold economic trade-offs involved. Finally, Section 6 concludes and derives recommendations for policies on cloud computing in the EU based on the preceding legal and economic analysis.

2. AN OVERVIEW OF CLOUD COMPUTING SERVICES AND THE EUROPEAN CLOUD COMPUTING INDUSTRY

2.1 Key Characteristics of Cloud Computing Services

Cloud computing is commonly defined as a "model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction".[9]

Hence, cloud computing services exhibit the following five essential attributes:[10]

- *On-demand self-service*: Computing resources can automatically be provisioned by a customer as needed (thus also termed 'on-demand administration').
- *Broad network access*: Resources are available over the network and can be accessed through standard access mechanisms that allow for the use of different end devices.
- *Resource pooling*: Computing resources of the provider are pooled to serve multiple customers using a multi-tenant model, that is, using shared infrastructure that allows for resources to be allocated dynamically to customer demand. In consequence, customers generally have no knowledge or control over the exact location of the provided resources ('sense of location independence').
- *Rapid elasticity:* Resources can be provisioned and released elastically, such that resources can scale quickly in accordance with the demand of the customer.
- *Measured service*: The usage of computing resources is automatically metered and can therefore be monitored, controlled, and reported by both the provider and the customer. Metered usage enables a payment model by resource units used ('pay-as-you-go').

This characterisation of cloud computing services has been similarly adopted in recent European legislation (see, for example, Article 6 (30) and Recital 33 NIS2[11]; Article 2 (8) and Recital 80 DA) and by national competition authorities in their cloud market studies.[12]

Cloud services are by now a key enabler of digital services and a vital infrastructure of the economy as a whole. They are therefore an important driver of innovation in the digital economy. Cloud services are regularly differentiated based on their employed *service model* that corresponds to the provision of infrastructures or services at a different layer of the 'cloud stack' (see also Figure 1 further below). In general, three service models are distinguished[13], although there also exist more granular typologies:

- *Infrastructure as a Service (IaaS)*: The customer can provision processing, storage, networks and other basic computing resources to install and run arbitrary software of their own choice.

[9] NIST (2011), The NIST Definition of Cloud Computing - Recommendations of the National Institute of Standards and Technology (U.S. Department of Commerce) by Peter Mell and Timothy Grance, p. 2.
[10] Ibid.
[11] Directive on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). [2022] OJ L 333/80.
[12] See, for instance, ACM, 2022 (n 5); Ofcom, 2023 (n 6).
[13] NIST, 2011 (n 9)

The customer bears responsibility for and has control over the operating system, storage and installed applications, but not the underlying infrastructure controlled and managed by the cloud service provider. Thus, IaaS denotes a service model at the lowest layer of the cloud stack.

- *Platform as a Service (PaaS)*: The customer can install applications of their own choice using programming languages, libraries, services, and tools supported by the cloud service provider. The customer has control over the installed applications and can possibly configure the application-hosting environment. The customer is responsible for the installation and maintenance of applications as well as data management. However, the customer does not control the underlying infrastructure, including the operating system and storage, which is controlled and managed by the cloud service provider. Thus, PaaS denotes a service model at an intermediary layer of the cloud stack.
- *Software as a Service (SaaS)*: The customer can use the application provided by the cloud service provider but has no control over the underlying cloud infrastructure and application-hosting environment, which are managed and controlled by the cloud service provider. In some cases, the customer may have control over limited application configuration settings. Thus, SaaS denotes a service model at the highest layer of the cloud stack.

Whereas IaaS and PaaS require the customer to develop or implement a significant part of the final service on their own, SaaS services can readily be deployed without much need for further development or implementation by the customer. Hence, cloud customers and business models differ considerably between IaaS/PaaS and SaaS.[14] Whereas IaaS and PaaS services are mostly used by customers with extensive IT expertise, SaaS services are used by a much broader customer base including consumers. In consequence, the SaaS services landscape is also much more diverse and differentiated than services at the PaaS layer and the IaaS layer.[15] PaaS is mainly used by application developers, for which PaaS helps to simplify development and deployment. Despite the intuitive conceptual characterisation of service models, a precise delineation is often difficult in practice, especially for the PaaS layer.[16]

2.1.1 Technical characteristics of cloud computing services

From a technological perspective, cloud services are currently characterised by a high rate of technical innovations and subject to continuous change in terms of both the available portfolio of services as well as the development and upgrading of existing services.[17] Recent major technical trends comprise the modularisation of software functions into micro-services (giving rise to the concept of serverless computing and 'Functions-as-a-service') and the integration of artificial intelligence (AI) and machine learning functions into services. As a result of service modularisation and functional encapsulation, customers of IaaS and PaaS services regularly provision a range of services fulfilling different functions that are then connected to an *ensemble of services* to support the workloads of the customer. For

[14] Autorité de la concurrence, 2023 (n 5)
[15] Autorité de la concurrence, 2023 (n 5); ACM, 2022, p. 53 (n 5)
[16] Ennis, S. F., & Evans, B. (2023). Cloud Portability and Interoperability under the EU Data Act: Dynamism versus Equivalence. Available at https://ssrn.com/abstract=4395183https://ssrn.com/abstract=4395183
[17] Schnurr, D. (2023). Switching and Interoperability between Data Processing Services in the Proposed Data Act. In: Data Act: Towards a Balanced EU Regulation. Centre on Regulation in Europe. https://cerre.eu/wp-content/uploads/2023/03/230327_Data-Act-Book.pdf

instance, a customer may combine a data storage service with computing services as well as a web server service. In this context, the term *multi-vendor cloud* (or *multi-cloud*) refers to customers combining services from different cloud service providers for different workloads instead of procuring all services from the same cloud service provider. In this report, we usually refer to multi-cloud in the narrower sense, meaning that services of different cloud providers are interconnected in order to create a service ensemble. This is different from the more general notion of a multi-cloud, where customers provision cloud services from different providers but each of these services run independently of each other.

Technically, the interconnection of services is enabled by the exchange of messages (that is, data flows) through application programming interfaces (APIs) that must be implemented and exposed by the individual services. APIs allow for a decoupling of the internal programming logic of a cloud service and the specified functions or input and output messages of the service. Interconnection requires *interoperability* between services, which can be achieved either by standardisation or by syntactic and semantic interoperability between services.[18] Syntactic interoperability refers to the ability to exchange data and semantic interoperability refers to the "ability to operate on that data according to agreed-upon semantics".[19] Syntactic interoperability is enabled by the exposure of an API and its accessibility by other services, whereas semantic interoperability requires a shared understanding between the services of the API's specification and functions. Interconnection of services is commonly feasible for services of the same cloud service provider but often more limited and difficult for services of different cloud service providers. [20]

A related but distinct technical concept from interoperability concerns *portability* of cloud assets, especially application portability and data portability. Whereas interoperability is usually necessary to interconnect different services, that is, is applied in vertical relationships between services, portability refers to a service provider's ability to transfer its cloud asset (such as its data or its application) to a different provider.[21] Thus, portability relates to horizontal relationships between services and is particularly relevant if a customer decides to switch between cloud services, as it facilitates the technical migration of a service to another cloud service provider.

2.1.2 Use cases, customers, and deployment models of cloud computing services

The *use cases* for provisioning cloud services as well as the types of cloud customers are highly diverse. A business customer may provision cloud services for *internal or external use* (see illustrations (c) and (d) in Figure 1). In external use cases, the cloud computing customer uses the cloud computing service as an input to develop and provide its own service to consumers. In internal use cases, the cloud computing customer itself is the consumer of the cloud computing service. In any case, the cloud service is provisioned as an input by the customer. Hence, the regular supply of cloud services follows

[18] Kaur, K., Sharma, D. S., & Kahlon, D. K. S. (2017). Interoperability and portability approaches in inter-connected clouds: A review. *ACM Computing Surveys (CSUR)*, *50*(4), 1-40.

[19] Rezaei, R., Chiew, T. K., Lee, S. P., & Aliee, Z. S. (2014). A semantic interoperability framework for software as a service systems in cloud computing environments. *Expert Systems with Applications*, *41*(13), 5751-5770.

[20] Ranjan, R. (2014). The cloud interoperability challenge. *IEEE Cloud Computing*, *1*(2), 20-24.

[21] See, e.g., for application portability Kolb, S., & Wirtz, G. (2014). Towards application portability in platform as a service. In *2014 IEEE 8th International Symposium on Service Oriented System Engineering* (pp. 218-229); International Organization for Standardization (2017). ISO/IEC 19941:2017 Information technology — Cloud computing — Interoperability and portability.

a 'pipeline model' along a vertical value chain and does not exhibit the typical characteristics of a 'platform model' (with the exception of cloud marketplaces as discussed further below).

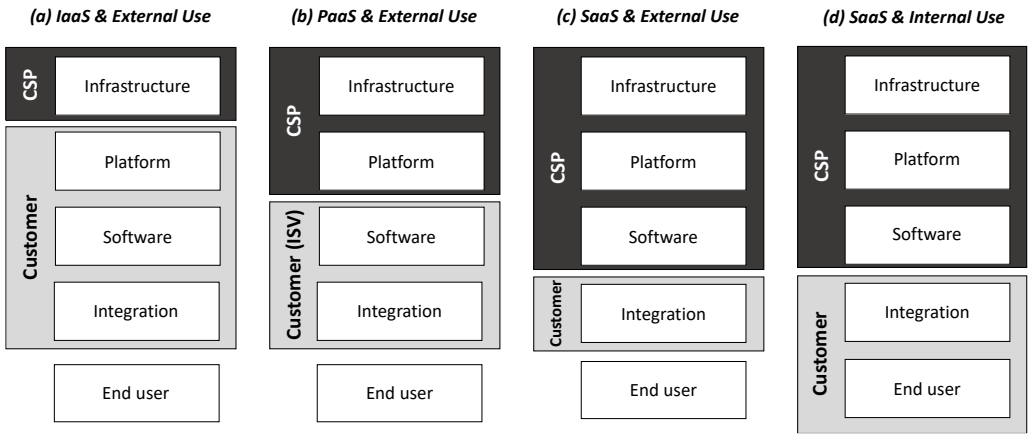

Figure 1: Illustration of cloud service models and provisioning for internal or external use.

Customers of cloud services comprise a range of very diverse users. In particular, cloud services may be used by business customers (that is, in B2B relationships) and consumers (that is, in B2C relationships). Consumers usually provision cloud services for a specific workload, for an individual user, and most commonly at the SaaS layer. In contrast, business customers (and other organisations) provision cloud services for a group of users (such as their employees), which frequently requires more sophisticated configuration of the service (for instance, for user authorisation). In addition, business customers have regularly higher demands on cloud services' security, reliability, and other quality of service features. Moreover, business customers frequently provision cloud services for different workloads and thus rely on several different cloud services that often also need to be interconnected. Depending on the needs and the IT expertise of the customer, business customers may not only provision services at the SaaS layer, but also at the PaaS and IaaS layer. Business customers and consumers typically, but not always, choose one service provider for a specific task. i.e., multi-homing for the same service is less common.[22] Thus, the design and features of cloud services may vary significantly based on whether they are meant to be used in B2B or B2C relationships.

Two categories of business customers can be distinguished.[23] The first group comprises businesses that have started their operations based on on-premises (non-cloud) infrastructure and are migrating their services and possibly infrastructures or a subset of them to the cloud. This can require complex technical transformation and re-design of a company's IT architecture, as illustrated by the eight year migration of Netflix's IT resources to the cloud.[24] In contrast, the second group comprises 'cloud-native organisations' that have grown in the cloud and are relying on the provisioning of their IT resources through the cloud from the beginning of their operations. Today, many start-ups are following the

[22] Autorité de la concurrence, 2023 (n 5).
[23] Ibid.
[24] Netflix (2016). Completing the Netflix Cloud Migration. https://about.netflix.com/en/news/completing-the-netflix-cloud-migration

cloud-native model, as this allows them to flexibly scale IT resources with demand and reduces the need for ex-ante fixed cost investments.

Independent software vendors (ISVs) represent a special type of business customers, as they rely on cloud service inputs (mostly IaaS services) to develop downstream services, such as PaaS or SaaS offerings.[25] At the same time, ISVs may compete with the SaaS offerings of cloud service providers when offering their own platforms or services as a Service. Furthermore, ISVs sometimes rely on cloud providers for the distribution of their services.[26]

Depending on the needs of a (business) customer, there exist different deployment models for cloud infrastructure and services:[27]

- In a *private cloud,* the cloud infrastructure is exclusively used by a single customer organisation. The infrastructure may be owned, managed, and operated by the customer, a third party, or some combination of them. The infrastructure may be located on the premises of the customer or off-premises.
- In a *public cloud,* the cloud infrastructure is provisioned for open use by the general public. The infrastructure is located on the premises of the cloud provider, that is, off-premises from the perspective of the customer.
- A *community cloud* is similar to a private cloud, but the cloud infrastructure is exclusively used by a community of organisations instead of a single organisation.
- A *hybrid cloud* integrates two or more distinct cloud infrastructures (most commonly private and public cloud) to enable data and application portability across these infrastructures.

According to Ofcom, the public cloud deployment model is adopted predominantly by customers that require scalability and flexibility to be able to adapt their business systems and to support innovations.[28] In contrast, the private cloud deployment model is used by customers who face mainly requirements with respect to latency, security, resilience, or regulatory compliance. The hybrid cloud deployment model is used when both sets of requirements must be accommodated or when legacy IT cannot be easily migrated to the cloud.[29] According to market research by Ofcom, hybrid cloud (combining private and public cloud) is the most common deployment model among IaaS and PaaS customers in the UK with a share of 44%. 34% of surveyed IaaS/PaaS customers reported that they only use private cloud, while 12% only use public cloud. 10% of customers use both private and public cloud but without an integration of the different infrastructures.[30]

In this report, the focus of our economic analysis is on business customers and public cloud services. In this context, we generally consider service models at all layers of the cloud stack, but highlight if differences in technical and economic characteristics between service models lead to different assessments and conclusions.

[25] See Ofcom, 2023 (n 6) and also illustration (c) in Figure 1.
[26] ACM, 2022 (n 5); Ofcom, 2023 (n 6).
[27] NIST, 2011 (n 9).
[28] Ofcom, 2023, p. 56 (n 6).
[29] Ibid.
[30] Ibid.

2.2 The European Cloud Industry

The cloud industry is experiencing significant growth with growth rates of about 30% per year in Europe in recent years.[31] In Europe, the majority of revenues are generated at the SaaS layer (61%), while PaaS (16%) and IaaS (22%) services also account for significant shares of total revenues and are expected to be particularly important drivers of future growth.[32] In 2021, 41% of all EU enterprises (with 10 or more employees and self-employed) used at least one cloud computing service with e-mail, storage of files, and office software as the most popular cloud services.[33] Thereby, the adoption of cloud services differs significantly between large enterprises (76%) and medium-sized and small enterprises (53% and 38%, respectively). Overall, cloud take-up in the EU increased by five percentage points compared to 2020.[34]

Cloud service providers that are present at all levels of the cloud stack have been commonly referred to as *hyperscalers* and offer a wide variety of cloud services at a large scale.[35] In Europe, the three largest cloud service providers in terms of market share, Amazon AWS, Microsoft Azure, and Google Cloud Platform, are usually referred to as hyperscalers.[36] The Netherlands Authority for Consumers and Markets (ACM) estimates that in the European Union, Amazon AWS and Microsoft Azure both have market shares of between 35% and 40%, while the market share of Google Cloud Platform is estimated at 5% to 10%.[37] In line with this assessment, Ofcom estimates that, at the IaaS layer, the three hyperscalers accounted for 70% to 80% of revenues associated with the supply of public cloud services in the UK.[38]

Besides the three hyperscalers, there are several other cloud service providers (such as IBM, Oracle, SAP, VMWare, OVHcloud, Scaleway) that provide services across different layers of the cloud stack.[39] Beyond providers active at different cloud layers, there exists a large number of providers that offer specialised services. This is especially the case for the SaaS layer with 25,000 to 30,000 SaaS providers in the market worldwide.[40]

The cloud industry also features a range of *suppliers of professional services* and *IT services companies* that provide complementary services and assume different roles in the relationship between business customers and cloud providers.[41] Most notably, these suppliers act as (i) system integrators of different cloud services for a customer, (ii) managed service providers, (iii) IT consultants that advise customers on cloud-related issues, or (iv) resellers of cloud services.

[31] ACM, 2022 (n 5).
[32] Ibid.
[33] Eurostat (2021). Cloud computing - statistics on the use by enterprises. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Cloud_computing_-_statistics_on_the_use_by_enterprises#Use_of_cloud_computing:_highlights
[34] Ibid.
[35] Ofcom, 2023 (n 6).
[36] ACM, 2022 (n 5); Ofcom, 2023 (n 6).
[37] ACM, 2022 (n 5).
[38] Ofcom, 2023 (n 6).
[39] ACM, 2022 (n 5).
[40] Ibid; Statista (2022). Leading software as a service (SaaS) countries worldwide in 2022, by number of companies. https://www.statista.com/statistics/1239046/top-saas-countries-list/
[41] Ofcom, 2023, p. 37 (n 6).

Next to their own cloud services, all hyperscalers offer *marketplaces*, through which customers can purchase PaaS and SaaS services developed by ISVs and other cloud providers.[42] According to Ofcom, 13% of all surveyed IaaS and PaaS customers in the UK mentioned that they were buying third-party services through the hyperscalers' marketplaces, although, 51% of respondents indicated that they were using marketplaces for some purpose (this may include, for instance, billing for existing services, buying the cloud provider's own services, or research and discovery of new services).

Two main types of contracts are common in the cloud industry:[43] First, standard contracts with prices commonly offered on the cloud service providers' website for an indefinite period and terminable at any time. Second, individually customised contracts that commonly specify a fixed contract length (most often with a contract length of two, three of five years in the case of IaaS and PasS)[44]. According to Ofcom, the latter is the predominant contract model for IaaS and PaaS services in the UK with only 17% of contracts on a pay-as-you-go basis.[45] In about 40% of these contracts between hyperscalers and IaaS or PaaS customers cloud services were bundled with other (non-cloud) products or services, whereas 56% were cloud-only contracts.[46]

Cloud computing services offer some major advantages for customers over traditional on-premises and outsourcing provision models for IT infrastructure and computing resources. Most notably, cloud services are rapidly scaleable and therefore allow for organisational agility as well as flexibility to quickly adapt to changes in customers' demand.[47] In addition, cloud computing can allow for significant cost savings (see, for example, the case of Netflix)[48] by benefitting from economies of scale in the provision of computing resources and avoiding inefficient under-utilisation of IT capacities. In particular, cloud computing drastically reduces the need for upfront capital investments as cloud computing services can be provisioned on a variable cost basis proportional to the utilisation of computing resources.[49] Moreover, in well-functioning cloud markets, competition can lower costs and yield quality improvements compared to on-premises solutions.[50] Furthermore, customers can benefit from increased specialisation, learning effects, and expertise of cloud service providers. In practice, customers' choice of a cloud provider is influenced by numerous factors. According to Ofcom, the main factors include i) quality and range of services, ii) pricing and costs, iii) ease of integration, iv) reputation and existing relationship, v) geographic reach, vi) security and resilience, vii) regulatory compliance, and viii) other factors.[51]

[42] ACM, 2022, p. 39 (n 5); Ofcom, 2023, p. 29 (n 6).
[43] Autorité de la concurrence, 2023 (n 5).
[44] Ofcom, 2023, p.47 (n 6).
[45] Ibid, p. 47.
[46] Ibid, p. 48.
[47] Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2011). Cloud computing—The business perspective. *Decision Support Systems*, *51*(1), 176-189. Makhlouf, R. (2020). Cloudy transaction costs: a dive into cloud computing economics. *Journal of Cloud Computing*, *9*(1), 1-11.
[48] Cloudzero (2023). Netflix Architecture: How Much Does Netflix's AWS Cost? https://www.cloudzero.com/blog/netflix-aws
[49] Marston et al., 2011 (n 47).
[50] Mahklouf, 2022 (n 47); Pal, R., & Hui, P. (2012). Economic models for cloud service markets. In *Distributed Computing and Networking: 13th International Conference, ICDCN 2012, Hong Kong, China, January 3-6, 2012. Proceedings 13* (pp. 382-396). Springer Berlin Heidelberg.
[51] Ofcom, 2023 (n 6).

3. REVIEW OF EU CLOUD POLICIES

3.1 Introduction: the EU Data Strategy

3.1.1 Data Strategy and cloud services

The current overall digital strategy started to be defined by the EU Commission (EC) at the end of 2020 with the Communication 'Shaping Europe's digital future', where the EC lays out the main pillars of its following five-year policy strategy.[52] In 2021, the EU Commission extended its sight to the next decade, presenting visions, targets, and setting out the paths to be followed toward digital transformation of Europe by 2030.[53]

Within the 2020 strategy, the Commission issued an additional specific thematic Communication concerning the 'EU data strategy', outlining a strategy for policy measures and investments to enable the data economy for the coming five years (2020-2025).[54]

The overarching general vision underlying the data strategy is that businesses and the public sector in the EU can be empowered by collecting, analysing, and using data to make better decisions, producing incremental value, and ultimately advantaging citizens and consumers. Therefore, an effective data strategy, data governance structure, and conducive data regulation are of pivotal importance for the economy and society.

The Data strategy policy pillars have been defined as follows: (i) empowering individuals, investing in skills and in SMEs; (ii) a cross-sectoral (horizontal) governance framework for data access and use; (iii) Common European data spaces in strategic sectors and domains of public interest; and (iv) investments in data and strengthening Europe's capabilities and infrastructures for hosting, processing, and using data.

The last of these pillars comprises access to competitive, interoperable, secure, and fair European cloud infrastructures and services. To this aim, the Commission data strategy aims to:

(i) **create a single European data space**, working as a single market for data, where **data can freely flow within the EU and across sectors** and cloud service providers comply with EU rules (such as the General Data Protection Regulation, or the Free Flow of non-personal Data Regulation);

(ii) incentivise (where relevant) the **adoption of self- and co-regulatory mechanisms and technological means** by cloud service providers aimed to increase trust, such as security by design and automated compliance;

(iii) establishing a comprehensive and coherent framework overview of all EU rules, including self-/co-regulatory schemes, available for cloud providers and users in the form of an **EU cloud rulebook**, offering a compendium of existing cloud codes of conduct and certification on security, energy efficiency, quality of service, data protection, and data portability;

[52] European Commission (2020) Communication "Shaping Europe's digital future"
[53] European Commission. (2021). Communication "Digital compass 2030—The European way for the digital decade".
[54] European Commission (2020) Communication EU data strategy

(iv) facilitate the **development of common European standards and requirements for the public procurement of data processing services**, thus enabling the EU's public sector at European, national, regional, and local levels to become a driver of new EU data processing capacities, rather than just a beneficiary of such European infrastructures;

(v) facilitate the set-up of **cloud services marketplaces at the EU level**, in order to: (a) connect demand-side organisations in the private (in particular SMEs) and public sectors to the new and innovative offering of tailored data processing services (specifically at PaaS and SaaS levels); (b) incentivise the compliance with a common and harmonised set of EU rules and requirements (including the use of transparent and fair contract conditions); and (c) address the market asymmetry between global actors, often offering integrated solutions containing applications also provided by smaller (EU) players;

(vi) establishing, by means of the European cybersecurity agency, **a European cybersecurity certification scheme for cloud services**, aimed to provide increased assurance to businesses, public administrations, and citizens that their data are secure wherever they are stored or processed;

(vii) establishing **a regulatory framework for a fair and competitive cloud market**, by tackling vendor lock-in, eliminating obstacles for switching between different cloud service providers, and boosting interoperability;

(viii) facilitating a gradual **move of cloud data and services to the edge,** while developing **interoperable cloud and edge services** to support the building of common **European data spaces**.

This programme about Cloud and Edge services and infrastructures is anchored in two objectives of the EU's Digital Decade, that is by 2030:

a. 75% of European businesses should use cloud-edge technologies for their activities;
b. 10,000 highly secure edge nodes should be deployed in the EU in order to provide the necessary connectivity and enable rapid data transfers.

After the definition of the EU data strategy, policy intervention at the EU level have tended to encourage data portability and switching through voluntary/co-regulatory initiatives, as defined by the Free flow of Data Regulation. However, these have been considered by the European Commission and some market players as not successful in terms of the outcome on market dynamics. Therefore, the Commission has initiated a number of diverse policy initiatives with a direct impact on competition and the well-functioning of the markets and the industry overall, going beyond the soft-law instruments and including binding legal requirements for cloud service providers, mainly in order to provide data portability and service interoperability. The main policy actions have resulted in the **Digital Markets Act** (DMA)[55] that addresses fairness and contestability issues for core platform services (CPS) including cloud computing services, and the **Data Act** (DA),[56] which specifically addresses switching and interoperability between providers of cloud, edge, and other data processing

[55] REGULATION (EU) 2022/1925 of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act)

[56] 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)

services. The EU Commission's intention is to further supplement these policy initiatives with forthcoming **Cloud Rulebook** and **Cloud marketplace initiatives**.

3.1.2 Free movement of data and data portability

Free movement and portability of data are considered fundaments for building a single digital EU market, where data, as an essential resource for economic growth, competitiveness, and innovation, can be fully exploited. Indeed, the free flow of data has emerged as the new cornerstone of European policy aimed at facilitating the development of innovative products and services that are more closely aligned with consumer preferences.[57] For the building of a single data market, EU legislation has primarily focused on removing barriers to the free flow of data across the internal market, safeguarding the fundamental rights of individuals with regard to personal data protection. Indeed, the elimination of obstacles for the free movement of data required additional specific safeguards for personal data, that is, "any information concerning an identified or identifiable natural person", which have been established by the **General Data Protection Regulation (GDPR)**.[58]

However, all digital data (personal and non-personal) can play a pivotal role for market contestability, growth and competitiveness,[59] the nature of the information resources valued in the data economy is often either personal in nature (that is, falling under the definition offered by the GDPR) or mixed in nature, where the boundaries of non-personal data are dynamically too fluid to make a clear distinction.[60] In addition, since a preponderant part of the information flows flowing through the European market are personal data, within the meaning of the broad definition provided in the GDPR, the portability of the same is a founding brick of the emerging 'common European data space'.

Nevertheless, the GDPR very notably includes among its purposes the free movement of personal data within the Union (Article 1.1), which may be "neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data" (Article 1.3). As a matter of fact, under the GDPR, ensuring a consistent level of protection of personal data and enhancing the free movement of personal data within the internal market are synergic objectives. The underlying principles are that, on one side, a poor (or geographically differentiated) level of rights to the protection of personal data may prevent the free flow of personal; on the other side, the proper functioning of the internal market requires that the free movement of personal data within the Union is not restricted for reasons connected with the data protection individual rights (Recital 13).

The objective of free movement of personal data has been mainly implemented within the GDPR by means of a general access and portability right, under Article 20, which brought a radical innovation in the landscape of data protection law in the European Union, adding a pro-competitive angle that

[57] EU Commission COM (2020) 66 final, A European strategy for data, p. 8.
[58] Article 4.1 of the GDPR: Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1 (GDPR).
[59] Cfr, CERRE The role of data for digital markets contestability: case studies and data access remedies
[60] Cfr. I. GRAEF, R. GELLERT AND M. HUSOVEC, Towards a Holistic Regulatory Approach for the European Data Economy: Why the Illusive Notion of Non-Personal Data is Counterproductive to Data Innovation, in TILEC Discussion Paper, No. 2018-028, September 2018, available at: http://ssrn.com/abstract=3256189, p. 10-11.

built the first enforcement connection between data protection and competition policy,[61] which is constantly growing.[62]

Indeed, in recent years, it has become evident that the underlying rationale behind Article 20 of the GDPR goes beyond mere control over personal data but reflects a clear pro-competitive goal of making information collected by incumbents in digital markets (social networks, online advertising services, online sales platforms, etc.) more contestable (Recital 68).[63] For these reasons, the right to data portability fits squarely within the framework of competition policies, differentiating itself from traditional data protection systems and instruments hinged on Article 8 of the EU Charter of Fundamental Rights.

With the introduction of such a right, the EU legal system intended to enhance the bargaining power of individuals by endowing them with more extensive control over their personal data, thus counterbalancing the asymmetric interaction between platform and users, and ultimately facilitating the change of service providers (switching). [64] Strengthening the control exercised by individuals over the processing of their personal data was intended to reinvigorate competition in digital markets where the collection, use, and processing of personal information plays a key role.

Under Article 20 GDPR, the data subject has the right to receive their personal data held by a controller and transmit it to another controller, or to have the data transmitted – where technically feasible – directly from one controller to another. Therefore, data controllers now enjoy a threefold right to data portability: (i) the right to receive a copy of the data provided to the controller, (ii) the right to transmit their data to a new controller, and (iii) the right to request the direct transfer of their data from the current controller to a new entity (Article 20). The first two rights can be freely exercised (as long as the process is based on consent or contract and is carried out automatically). The exercise of the third right depends largely on its technical feasibility, that is, the interoperability of the underlying interface (Recital 68).

These rights, being part of the broader GDPR framework, which is a horizontal and symmetric regulation, can be brought against any data controller regardless of the controller's turnover, business model, market power, as well as the reasons for requesting portability or the burden on the controller in fulfilling the request.

[61] Indeed, with the relevant exception of the payment account access rule provided in PSD2, there had been no such regulatory initiatives before GDPR. Cfr. Borgogno O., Manganelli A. (2021) Financial Technology and Regulation: The Competitive Impact of Open Banking in Market and Competition Law Review, volume V, 2021(1), 105- 139.

[62] Starting from the significant case Facebook v. Bundeskartellamt, and the consequent recent ECJ preliminary ruling decision, where the preliminary question concerns both the antitrust authority's jurisdiction to detect a GDPR violation as well as whether the compliance or not for dominant player with the GDPR rules may be an important indication/factor of whether there could be an abuse of dominant position.

[63] Cfr. O. LYNSKEY, Aligning data protection rights with competition law remedies? The GDPR right to data portability, European Law Review 793, 2017, 803. F. Costa-Cabral, O. Lynskey, Family ties: The intersection between data protection and competition in EU law, Common Market Law Review, No. 54/1, 2017, 11-50.

[64] Article 29 Data Protection Working Party, Guidelines on the right to 'data portability', 2017.

Of course, Cloud Computing services may well process[65] personal data, and therefore may fall within Article 20 GDPR scope of application, as far as they can be qualified as data controllers or data processors. However, the exercise of this right, and its pro-competitive impact, has been rarely exercised and proven largely ineffective.[66]

First of all, it does not entitle the data subject to continuous or real-time access to the data, which is important for products and services that are always connected to the internet;[67] moreover, Article 20.1 of the GDPR does not provide detailed guidance on how to ensure portability of data between businesses[68] and any attempt to mandate the adoption of interoperable standards is ruled out as Recital 68 of the GDPR does not go beyond mere 'encouragement'; finally, the limitation to personal data of such obligations for data controller or processors made the GDPR not such an effective pro-competitive tool for cloud services (compared to other digital services and markets where personal data are monetised either by means of advertising or by differentiating products and services on the basis of consumers' preferences).[69]

As far as non-personal data are concerned, the EU approved the **Free Flow of Non-Personal Data Regulation**[70] that applies to natural or legal persons who provide data processing services to users residing or having an establishment in the Union. Here, data processing is meant in the broadest sense, encompassing the usage of all types of IT systems, whether located on the premises of the user or outsourced to a service provider. It covers data processing of different levels of intensity, from data storage (IaaS) to the processing of data on platforms (PaaS) and in applications (SaaS) – as defined in the introductory Section 1.

The Regulation ensures:

- free movement of non-personal data across borders: every organisation should be able to store and process data anywhere in the EU;
- the availability of data for regulatory control: public authorities will retain access to data, even when it is located in another EU country or when it is stored or processed in the cloud;
- easier switching between cloud service providers for professional users.

Therefore, its overarching objective is to ensures that non-personal data can be stored, processed, and transferred anywhere in the EU.

[65] Under GDPR 'processing' means "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction". (Article 4(2))

[66] Cfr. Syrmoudis, E., Mager, S., Kuebler-Wachendorff, S., Pizzinini, P., Grossklags, J., & Kranz, J. (2021). Data Portability between Online Services: An Empirical Analysis on the Effectiveness of GDPR Art. 20. Proc. Priv. Enhancing Technol., 2021(3), 351-372; EU Commission (2022) Final report - sector inquiry into consumer Internet of Things

[67] Cfr. Krämer, J. (2021). Personal data portability in the platform economy: economic implications and policy recommendations. Journal of Competition Law & Economics, 17(2), 263-308; and CERRE Making data portability more effective for the digital economy.

[68] The GDPR simply states a general requirement for the format of transmitted data, which must be "structured, commonly used and machine-readable."

[69] Cfr. Manganelli A., Nicita A. (2021) Regulating digital platforms: The road ahead in Competition policy in the digital economy, May 2021, Concurrences N° 2-2021, Art. N° 100010.

[70] REGULATION (EU) 2018/1807 of 14 November 2018 on a framework for the free flow of non-personal data in the European Union

To this end the regulation establishes a general prohibition of data localisation requirements, that is, Member States (as well as regional or administrative authority and municipality) cannot compel the location of data in a specific geographical area or territory in the EU (or outside) for the purpose of data processing, unless they are justified on grounds of public security in compliance with the principle of proportionality (Article 4).

Besides public rules, data mobility can also be inhibited by private restrictions: that is, legal, contractual, and technical issues hindering or preventing users of data processing services from porting their data from one service provider to another or back to their own information technology (IT) systems, not least upon the termination of their contract with a service provider (Recital 5). For this reason, the regulation also addresses the problem of 'vendor lock-in' at the level of providers of data processing services, by mandating the Commission to encourage the introduction of self-regulatory codes of conduct that facilitate switching data between cloud services.

According to Article 6.1, those codes should be based on the principles of transparency and interoperability and take into due account open standards, covering:

- best practices for facilitating the switching of service providers and the porting of data in a structured, commonly used, and machine-readable format including open standard formats where required or requested by the service provider receiving the data;
- minimum information requirements to ensure that professional users are provided, before a contract for data processing is concluded, with sufficiently detailed, clear, and transparent information regarding the processes, technical requirements, timeframes, and charges that apply in case a professional user wants to switch to another service provider or port data back to its own IT systems;
- approaches to certification schemes, including quality management, information security management, business continuity management, and environmental management, aimed to facilitate the comparison of data processing products and services for professional users;
- communication roadmaps taking a multi-disciplinary approach to raise awareness of the codes of conduct among relevant stakeholders.

In response, industry participants developed the 'SWIPO' (switching cloud providers and data porting) codes of conduct. However, according to the EU Commission,[71] those codes have been adopted just by a few providers and they are not completely compliant with the Regulation requirements as they are mostly focused on pre-contractual transparency, lacking to consider and tackle all the technical and economic obstacles, thus not having had a significant positive impact on market dynamics. This posed the ground for the development of the Data Act. In this regard, however, the development of a voluntary code could have represented a necessary first step toward the definition of effective rules and procedures.

[71] EU Commission Staff Working Document (2022) IMPACT ASSESSMENT REPORT Accompanying the document Proposal for a Regulation on harmonised rules on fair access to and use of data (Data Act)

3.2 Data Act

3.2.1 Legislative objectives and structure

A proposal for a Data Act was put forward by the EU commission in February 2022, in June 2023 a compromise position was reached by the co-legislators, upon which on 9 November the European Parliament approved its legislative resolution which has been ratified by the Council on 27 November 2023 with no further amendments. This piece of legislation aims to represent a key pillar of the European Strategy for Data in which the Commission announced the establishment of EU-wide common, interoperable data spaces.[72] In particular, it aims to achieve the following **objectives:**

- to **facilitate access to and the use of data by consumers and businesses**, while preserving incentives to invest in ways of generating value through data;
- to **provide for the use by public sector bodies and EU institutions of data held by enterprises** in certain situations where there is an **exceptional data need**;
- to **provide for the development of interoperability standards for data to be reused between sectors**, in a bid to remove barriers to data sharing across domain-specific common European data spaces and between other data that are not within the scope of a specific common European data space.

Specifically, for data processing services including cloud and edge services, the Data Act builds on the rules related to the free flow of data, and also specifically on the provision in Article 6, which encourages codes of conduct to facilitate the porting of data and the switching between cloud providers.

According to the DA's Impact Assessment, as well as national investigations described at section 3.6, markets for cloud and edge services are not sufficiently competitive, as they are very concentrated (especially for IaaS) and the ability for customers to switch from one data processing service to another is very limited, as the self-regulatory approach promoted by the Free flow of non-personal data Regulation has been largely ineffective so far (Recital 79).

Based on this premise, the DA introduces legally binding and detailed obligations aimed at:

- removing obstacles for switching providers of data processing services of the same service type (Chapter VI);
- enabling/facilitating interoperability between providers of data processing services of the same service type (Chapter VIII);

Moreover, the DA prescribes data processing providers to put in place safeguards against unlawful international and third-country governmental access and transfer of non-personal data (Chapter VII), which however does not fall within the scope of this report, focusing on competition-related issues.

Switching and interoperability obligations apply to data processing services (DPS),[73] comprising and directly aiming at cloud computing and edge services, falling into one or more of the following three

[72] Cfr. In general about Data Act, CERRE (2023) DATA ACT: Towards a Balanced EU Data Regulation

[73] The DA defines a DPS as "a digital service enabling ubiquitous, and on-demand network access to a shared pool of configurable, scalable and elastic computing resources of a centralised, distributed or highly distributed nature, provided to a customer, that can be rapidly provisioned and released with minimal management effort or service provider interaction" (Article 2.12).

data processing service delivery models: IaaS (infrastructure-as-a-service), PaaS (platform-as-a-service) and SaaS (software-as-a-service) (Recital 81).

The DA applies to all data processing services, and its Chapters VI and VII appear to target cloud computing services primarily and therefore can almost be considered as a sector-specific regulation, as dealing with specific services (that is, a specific industry), especially in comparison with the Digital Markets Act covering a range of different digital markets and services. This would create an explanation as to why the DA provisions of Chapters VI and VII are more detailed and specific than the DMA and could also give them a higher interpretative (that is, derogative) force in case of normative overlaps and antinomies. On the other hand, as far as DPS switching and interoperability provisions, the DA provides a symmetric regulatory framework, applied to all providers regardless of their size, customer base, market share, or market power, whereas the DMA provides an asymmetric regulation that only applies to certain gatekeeper platforms. Normally, one would expect the symmetric regulatory framework to be less heavy-handed than the asymmetric regulatory framework (cfr. the telecommunications framework under EECC which consists of symmetric rules applicable to all, and asymmetric rules applicable to players with significant market power, for instance). From that perspective, it is quite surprising to see that the DA goes beyond the DMA when it comes to portability and interoperability.

Finally, in its introductory part, in line with the general EU Data strategy, the DA states that interoperability and switching between DPS should be accompanied by the use of implementation and/or compliance tools, notably those published by the Commission in the form of the **Rulebook for cloud services**. (Recital 96). In addition, the DA also recommend the use of voluntary **standard contractual clauses**, developed by relevant bodies or expert groups established under Union law, which are considered beneficial to increase confidence in DPS, as well as improve legal certainty on the conditions that apply for switching. Neither the Rulebook nor standard contractual clauses have been issued yet.

3.2.2 General rules and rationales about switching and interoperability.

Chapter VI of DA aims to remove obstacles to effective **switching from one DPS provider to another one** that covers the **same service type** or, where relevant, to **use several providers of DPS**. Therefore, the obligation seems to extend not only to **a switching process** (passing from provider A to provider B) but also aims to facilitate the **adoption of a multi-cloud approach**.

A narrow multi-cloud setting, when referred to service of the same type, as described in the introduction, seems to be quite rare. However, in places, the DA does not explicitly refer to services of the same service type, implying that it could apply more generally to all DPS, having some complementarity features. Here, the definition of 'same service type' becomes relevant, interplaying with the complementarity/substitutability relationship between services.

Article 2.9 defines '**same service type'** as a "set of data processing services that **share the same primary objective**, data processing service model, and **main functionalities**". Services falling under the same service type may share the same data processing service model (IaaS, PaaS, or SaaS) however, two databases might appear to share the same primary objective, but after considering their

data processing model, distribution model, and the use cases that they are targeted at, such databases could fall into a more granular subcategory of similar services.[74] Services of the same service type may have different and competing characteristics such as performance, security, resilience, and quality of service. (Recital 81).

Thus, Recital 81 seems to imply that 'same service type' could be quite related to a concept of **substitutability on the demand side.** This suggests that services using the same data processing model might not belong to the same category but could have complementary features. This, from an economic standpoint, could support the need for interoperability in a multi-cloud setup where different data processing services with complementary functions are used simultaneously. However, it appears that the current definition of service types lacks the precision required for effective enforcement of data regulation.

Chapter VIII (comprising Articles 33, 34, and 35) generally deals with interoperability obligation, and Article 2.40 defines 'interoperability' as "the ability of two or more data spaces or communication networks, systems, connected products, applications, data processing services or components to exchange and use data in order to perform their functions".[75]

Moreover, in a specific situation, **unbundling a particular service from the overall service supplied by the original DPS provider and moving it to another provider can also be considered as switching** (Recital 85). Indeed, Recital 93 specifies that "providers of data processing services should also be required **to remove obstacles to unbundling a specific individual service from other data processing services** provided under a contract and **make the relevant service available for switching**, **in the absence of major and demonstrated technical obstacles that prevent such unbundling**." In line with this, Article 23.1 requires DPS providers to also eliminate obstacles for the unbundling of IaaS services, where technically feasible, from other data processing services.

This provision is hard to decipher: in an extensive interpretation, this might create the economic rationale for a vertical interoperability, allowing customers to move an entire data processing service from one provider to the other, that is, allowing a **service portability. However, considering the other provisions around 'functional equivalence' and the caveats placed on a cloud provider's ability to facilitate switching, it should most probably be interpreted as just referring to an obligation to make two services available as stand-alone services.**

As for the switching process itself, Article 2.34 defines it as "the process involving a source provider of data processing services, a customer of a data processing service and, where relevant, a destination provider of data processing services, whereby the customer of a data processing service changes from using one data processing service to using another data processing service of the same service type,

[74] Cfr. Ennis & Evans, 2023 (n 16).

[75] This could be defined 'horizontal interoperability' when the exchange and use of data take place between services of the same service type or at the same level of the vertical value chain, or 'vertical interoperability' when the exchange and use of data take place between services at a different level of the value chain. Differentiation between horizontal and vertical interoperability are valuable for understanding the concept theoretically. However, practical implementation and the dynamic nature of technology should be considered when addressing interoperability challenges in real-world scenarios.

or other service, offered by a different provider of data processing services, or to an on-premises ICT infrastructure, including through extracting, transforming and uploading the data".

During switching customers can ask to transfer data to another provider, as well as to switch to an on-premises infrastructure,[76] as well as to delete data and exportable assets. Switching rights for customers can be applied also for mere termination (not passing to another provider) when the customer asks for the deletion of data (Recital 85).

During the switching process, the DA clarifies that the responsibility for switching to another data processing service (DPS) provider would apply only to the "services, contractual agreements and practices" provided by the source provider (Article 24). Indeed, providers of data processing services and customers have different levels of responsibilities, depending on the steps of the process referred to. For instance, the source provider of data processing services is responsible for extracting the data to a machine-readable format, but it is the customer and the destination provider who will upload the data to the new environment, unless a specific professional transition service has been obtained (Recital 85). In this context, Article 27 defines a **general good-faith and cooperation obligation** for all parties involved in the switching process in order to guarantee its effectiveness, enable the timely transfer of data and maintain the continuity of the service. In this regard it should be noted, as highlighted above, that there are different 'switching' or 'interoperability' scenarios and therefore the timely transfer of data depends on the specific scenario, making it hard to determine an effective 'one size fits all' solution.

In this regard, a partially different regulatory treatment is defined for '**custom-built DPS**', which will be examined next. For custom-built DPS, the DA means those DPS where **(i)** the majority of features have been custom-built to accommodate the specific needs of an individual customer or where all components have been developed for the purposes of an individual customer, **and (ii)** are not offered at broad commercial scale via the service catalogue of the data processing service provider. Prior to the conclusion of a contractual agreement on the provision of **custom-built DPS**, the provider must inform the prospective customer of the obligations that do not apply to the respective service (Article 26a).

Obstacles are not well defined, however, and are simply referenced according to different types: commercial, technical, and economic. They restrain the ability of customers regarding:

- Termination of the contract and switching charges (although providers and customers can agree on fixed term contracts)
- Conclusion of a new contract of the same service type
- Porting of data
- Achieving functional equivalence for 'infrastructural services'
- Unbundling (where technically feasible) for 'infrastructural services'
- Interoperability for Paas and SaaS

[76] Meaning "an ICT infrastructure and computing resources leased, rented or owned by the customer, located in its own data centre and operated by the customer or by a third-party" (Article 2(33)).

Those obstacles should be removed, according to Article 23, by complying to obligations disciplined by Articles 25, 26, 27, 29, and 30, described below, which define and impose consumer protection and empowerment tools, related to contractual terms of DPS, contractual transparency, information duties, and a good-faith general obligation. Those provisions are then supplemented or specified by the obligations at Articles 33, 34, and 35 (**Chapter VIII**).

Generally speaking, Chapter VI and Chapter VIII of the DA introduce far-reaching potentially impactful – whether negative or positive – relevant provisions, however those provisions should definitely be further clarified, made internally coherent, primarily by better specifying the concepts of data portability and interoperability (vertical and/or horizontal), their respective scopes of application and their possible interplays.

3.2.3 Termination of the contract and conclusion of a new contract

In order not to restrain effective switching Article 23 and Article 25 DA mandate DPS providers to include specific clauses concerning the termination of the contract in their contract with customers.

In general, termination takes place after a notice period and the successful finalisation of the switching process. In particular, the contract must include a maximum two-months' notice period for the initiation of the switching process, after which the user may notify the Data Processing Service Providers (DPSP) of its decision to (a) switch to another provider; (b) switch to an on-premise system; (c) delete its digital assets and exportable data. Therefore, termination takes place and is notified: (i) when the switching process is completed; (ii) right after the notice period if the user does not want to switch but delete data and digital assets (mere termination).

If the user wants to switch: the source provider must (a) not create obstacles for concluding new contractual agreements with a different provider of data processing services covering the same service type; and (b) complete the technical aspects of the switching process within a maximum 30-day transition period (starting after the ending of the notice period). During the transition period, the service contract remains applicable, and the provider must assist users, keep them informed about the switching process and be responsible for the security of data. This transition period can be extended by the user once for a period that the user considers appropriate for its own ends. Where the 30-day mandatory transition period is technically unfeasible, the DPSP informs the customer within 14 working days after the switching request has been made and shall duly motivate the technical unfeasibility and indicate an alternative transition period, which may not exceed 7 months during which service continuity must be ensured against reduced cost-oriented charges (referred to in Article 29(2).

It is important to clarify that the DA does not prevent establishing a contractual relationship with a fixed duration (possibly tacitly renewable) defined by the contract (Recital 89). Coherently, the same contract can impose a **proportionate early termination fee** that, according to general EU consumer protection provisions, compensates for early termination of the contractual relationship. Such an early termination fee is considered by the DA something different from a switching fee (that comprises

egress fee).[77] However, before entering into a contractual agreement with a customer, providers of data processing services shall provide the prospective customer with clear information on standard service fees and early termination penalties that might be imposed on the customer (Article 25.3a)

In the same vein, the DA does not impose any maximum contract length, as is the case for sector-specific consumer protection legislation in other sectors (such as the EU code for electronic communications).

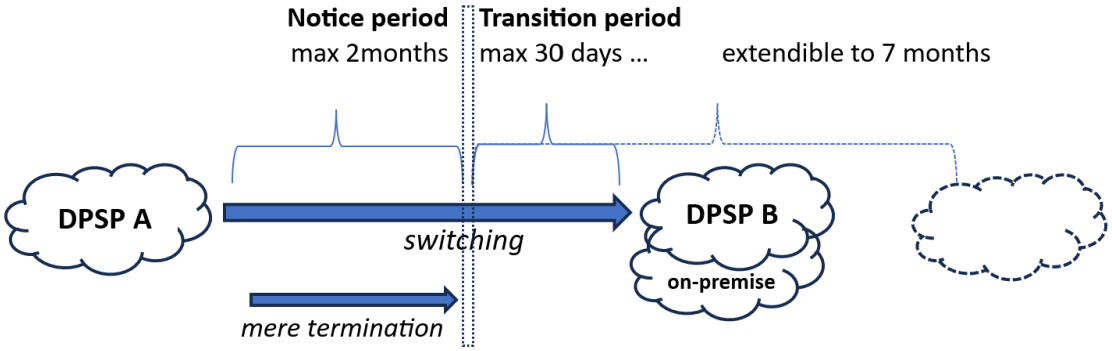

Figure 2: Illustration of provisions on termination and switching.

3.2.4 Switching charges and egress fees

Article 25 deals with charges imposed by data processing providers on their customers for the switching process (that is, switching charges), including data egress charges, that are related to the transit of data from one provider to another provider or to an on-premises system (leased, rent, or owned by the customer).

The DA imposes a reduction and eventual complete withdrawal of switching charges. In particular, a) from the date of the DA's entry into force DPSP can impose a switching charge not exceeding the costs incurred by the provider of data processing services that are directly linked to the switching process concerned (cost-oriented charges), and (b) maximum 3 years after the DA's entry into force any DPSP must end requiring switching charge to users. This information should be clearly provided by DPSP before entering into a contractual agreement with a customer.

Within the DA Article 29 considers all switching charges to be an economic obstacle to switching, even if, in general, Recital 88 stresses how only "unnecessarily high data egress charges and other unjustified charges unrelated to actual switching costs" have the potential to limit competition and cause lock-in effects for the customers. As a matter of fact, in general, cost-oriented charges, if known ex-ante by consumers, should not alter in an anti-competitive way their decision-making about switching. However, it is quite difficult for customers to estimate upfront the volume of data that they will have to transfer. Therefore, even if prices may be transparent, they can hardly be predicted (see

[77] Indeed, Article 2.13d defines 'switching charges' as "charges, other than standard service fees, imposed by a data processing provider on a customer for the actions mandated by this Regulation for the switching to the systems of another provider, and other than early termination penalties." Switching charges also include data egress charges defines as "data transfer fees charged to the customers of a provider of data processing services for extracting their data through the network from the ICT infrastructure of a provider of data processing services to the systems of another provider or to on-premise infrastructures" (Article 2.13(c))

section 4.1 for a further discussion from an economic perspective). This provision is aimed to further enhance switching and competitive pressure on all providers, however, a regulatory obligation to eliminate any charge could result in a passing-on of switching costs on the standard service fees, which a larger operator could dilute onto a larger customer base. On the other side, this would allow to compare prices in a more transparent, understandable, and predictable way.

This provision does not apply to **custom-built DPS**. The economic rationale relies on the specific costs/investment that the DPSP may have done for designing and implementing a tailored specific service. However, where relevant, providers of data processing services shall provide information on services that involve highly complex or costly switching or for which it is impossible to switch without significant interference in the data, digital assets, or service architecture.

Finally, it is important to underline that **standard service fees for the provision of data processing services are not considered switching charges**. Therefore, these standard service fees are not subject to withdrawal and remain applicable until the contract for the provision of the respective services ceases to apply. Consequently, in case customers request additional services that go beyond the switching obligations for DPSP (as described in DA Chapter VI), these additional services can be supplied and charged by the DSPS (Recital 89).

Article 29 shall also apply, *mutatis mutandis*, in relation to data egress charges to facilitate interoperability for the purposes of in-parallel use of data processing services, and in particular data egress charges could be maintained, in a cost-oriented fashion, even beyond the Article 29 transition period (Article 34.2). According to the DA, this different treatment is justified by the fact that, within in-parallel use of services, the egress of data can be an ongoing activity and not a one-off activity. Therefore, it would be disproportionate to prohibit DPSPs from charging consumers to cover costs (Recital 99).

3.2.5 Porting of data

In order to facilitate switching, avoid unnecessary and burdensome tasks, and to ensure that the customer does not lose any of their data as a consequence of the switching process, DPSPs must eliminate obstacles to allow the porting of the customer's exportable data and other digital assets to another provider of data processing services or to an on-premises infrastructure, including after having benefited from a free-tier offering.

Moreover, DPSPs should inform the customer ahead of switching of the scope of the data that can be exported to a different provider or be moved to an on-premises infrastructure.

The scope of exportable data should include at a minimum "input and output data, including metadata, directly or indirectly generated, or cogenerated, by the customer's use of the data processing service" (Article 2.38, Recital 82), in addition to 'digital assets', that are "elements in digital format, which the customer has a legitimate right of use, independently from the contractual relationship of the DPS, e.g., applications and metadata related to configuration of settings, security, and access and control rights management, and other elements such as manifestations of virtualisation technologies, including virtual machines and containers" (Article 2.32, Recital 83). The scope of this definition might be considered somehow very broad, as done without a specific

assessment of which non-directly generated data, when ported, could reduce switching costs for customers, especially considering that the DA, unlike the DMA, is a symmetric regulation, and extra costs imposed on all providers (also small ones) should be careful assessed.

From the exportable data the following can be excluded: (a) data and digital assets belonging to DPSPs or to third parties, (b) DPSP data protected by intellectual property rights or constitutes trade secrets of that provider, and (c) third party's assets or data related to the integrity and security of the service, the export of which will expose the DPSP to cybersecurity vulnerabilities. All these exclusions should not impede or delay the switching process (Recital 82). For this reason, the contract must include an exhaustive specification of categories of data specific to the internal functioning of the provider's services that will be exempted from the exportable data, where there is a risk of breach of trade secrets.

Moreover, the contract must include a minimum period of 30 days for data retrieval, starting after the end of the transition period, after which – if not agreed differently and if the switching process was completed successfully – all exportable data and digital assets must be erased.

As described in the previous paragraphs, Article 25 defines some pro-competitive and consumer empowerment actions, related to contractual features and contractual transparency. Article 26, in turn, imposes post-contractual information duties on DPSPs in order to support the customer's exit strategy.

Article 26 states that DPSPs have to (i) inform users of available procedures for switching and porting to the data processing service, including information on available porting methods and formats as well as restrictions and technical limitations that are known to the provider of destination data processing services; (ii) provide users with reference to an up-to-date online register hosted by the data processing service provider, with details of all the data structures and data formats as well as the relevant standards and open interoperability specifications in which the exportable data will be available.

3.2.6 Functional equivalence and unbundling for IaaS services.

In the switching process, **for DPS of IaaS services**, the DA aims to allow customers to achieve **functional equivalence** in the use of a DPS of a destination provider or providers, when covering the same service type...

According to the DA, 'functional equivalence' means re-establishing, based on the customer's exportable data and digital assets, a **minimum level of functionality of a service** in the environment of a new DPS of the same service type after switching, where **the destination service delivers a materially comparable outcome for the users in response to the same input** for shared features supplied to the customer (Recital 86 and Article 2.37).

Consistently with the general principle in Article 24, stating that the responsibility for switching to another DPS provider would apply only to the "services, contractual agreements and practices" provided by the source provider, as for the functional equivalence requirement**, DPS providers are expected only to facilitate functional equivalence for the features that both the source and**

destination services offer independently. Namely, DPS providers must take in good faith "**all reasonable measures in their power to facilitate the achievement of functional equivalence in the use of the destination service**", by providing capabilities, adequate information, documentation, technical support and, where appropriate, the necessary tools (Article 30.1).

Therefore, the DA does not require DPS providers to develop new categories of data processing services or to rebuild the service in question within the destination provider's infrastructure (to which the source provider does not have access) in order to facilitate functional equivalence in an environment other than their own systems (Recital 92). For this very reason, the functional equivalence requirement does not apply to **custom-built DPS** (Article 31). Indeed, generally, it would be unfeasible or very burdensome to facilitate functional equivalence for DPS enjoying specific customised features.

This interpretation of functional equivalence should represent a safeguard for the innovation process, as all providers would not be required to deliver similar services. In any case, even with some of the clarity introduced regarding custom-built DPS, this concept could prove very difficult to operationalise and could likely generate a high level of controversies and litigation before a consolidated (administrative or judicial) case-law is built, which would be a long process, also considering the highly decentralised DA enforcement framework (section 2.8).

On a different perspective, as mentioned, the DA aims to facilitate for unbundling of infrastructural services, where technically feasible (Articles 23, 23e and Recital 93).

Under this light, the functional equivalence requirement might acquire a slightly different meaning, referable to the vertical relationship between DPS providers in their competitive process. Indeed, where a provider is vertically integrated across different data processing service models and a downstream competitor has to 'access' upstream DPS, at IaaS level, functional equivalence could be interpreted and applied also as an 'equivalence of access' requirement, which would work as a non-discriminatory obligation aimed to inhibit self-preferencing actions by the vertically integrated DPS provider. In such a framework, this regulatory requirement, would resemble an 'equivalence of outputs' concept as it is applied in the electronic communications sector, where the services offered upstream by a vertically integrated operator to other operators and its own downstream unit are comparable in terms of functionality and price, although different systems and processes may be used.[78]

However, in the telecom sector, this obligation is imposed only on operators enjoying a significant market power (which is like a dominant position). Indeed, such an obligation, would be very onerous, considering not only the vast differences between the two markets – telecoms and cloud – but also that the DA establishes a symmetric regulatory framework that is applied to all DPS providers, regardless of their scale and market power. Imposing regulatory requirements across DPSs IT risks making it harder for smaller providers to innovate new technological solutions, differentiate

[78] In the Electronic communications framework, there is also a more stringent concept for implementing the equivalence of access/non-discrimination obligation. That is the "equivalence of inputs" and require applying exactly the same prices and processes to upstream services offered to competitors and for the downstream unit of the vertically integrated operator.

themselves, and thereby compete. Unlike telecoms where providers offer customers the same basic set of services and can therefore operate under uniform standards and enable direct customer switching, IT providers offer a far wider array of different functions and features and compete fiercely on innovation to differentiate their products to meet customer needs. IT providers are constantly launching new features, new services, and new service categories.

3.2.7 Interoperability for PaaS and SaaS

As mentioned, the DA is based on the consideration that "an ambitious and innovation-inspiring regulatory approach **to interoperability is needed to overcome vendor lock-in**, which undermines competition and the development of new services." (Recital 89) Open interoperability specifications and harmonized standards are expected to **enable a multi-vendor cloud environment**, which is considered by the European Commission as a key requirement for open innovation in the European data economy. However, the DA explicitly recognises that enhanced contestability must not come at the price of a negative impact on the security and integrity of services and data, or hinder technical advances and inclusion of new functions and innovation in data processing services (Recital 100 and Article 35.1).

Instead of the concept of functional equivalence applied to IaaS to ease the switching process, Article 30 defines for PaaS and SaaS a general interoperability obligations. In particular, Article 30.2 requires providers of PaaS and SaaS services "to make **open interfaces publicly available and free of charge** to facilitate switching", and Article 30.3 requires them to "ensure compatibility with common specifications based on **open interoperability specifications** or **harmonised standards for interoperability"** referring to central Union data processing service standards repository. The latter does not apply to **custom-built DPS**.

Within the DA 'harmonised standard' means a harmonised standard as defined in Article 2, point (1)(c), of Regulation (EU) No 1025/2012, whereas 'open interoperability specifications' refer to ICT technical specifications, as defined in Regulation (EU) No 1025/2012, which are performance-oriented towards achieving interoperability between data processing services (Articles 2.41 and 2.43).

Article 30.4 states that if open interoperability specifications or harmonised standards have not been identified in the central Union data processing service repository, the DPSP must, "at the request of the customer, export all exportable data in a structured, commonly used and machine-readable format." This last 'second-best' obligation aims to facilitate the one-off data import and export for the purpose of switching providers, in line with the general data porting obligation at art 23 for all IaaS, PaaS, and SaaS, when interoperability is not facilitated by the centralised definition of specifications and standards.

Article 34 states that those requirements in Articles 30.2, 30.3, 30.4 are also applicable, *mutatis mutandis*, to providers of data processing services **to facilitate interoperability for the purposes of in-parallel use of data processing services**. Thus, this provision seems to be finally distinguishing between a horizontal interoperability, covered by Article 30, and a vertical interoperability, covered by Article 34.

According to Article 34, requirements in Articles 23, 24, and 25.2 (points (a)(ii), (a)(iv), (e) and (f)), must also be applied for interoperability. In particular, as described in the previous sections, Article 23(1) concerns the elimination of obstacles that inhibit consumers from (a) terminating the contractual agreement; and (b) concluding a new contractual agreement; (c) porting the customer's exportable data, other digital assets to another DPSP; (d) achieving functional equivalence for services of the different provider covering the same service type; and (e) unbundling, where technically feasible, infrastructural services from other DPSs. Provisions at Article 25.2 concern the referral in the contract of (i) acting with due care to maintain business continuity, and continue the provision of the respective functions or services under the contract; (ii) providing clear information concerning known risks to continuity in the provision of the respective functions or services on the part of the provider of source data processing services; (iii) an exhaustive specification of all categories of data and digital assets that can be ported during the switching process, including, at a minimum, all exportable data; (iv) exhaustive specification of categories of data specific to the internal functioning of provider's service that will be exempted from the exportable data, where a risk of breach of trade secrets of the provider exists.

Therefore, on the one hand, vertical interoperability is required for effective service portability. On the other hand, interoperability of DPSs of different providers that are not of the same service type would also allow to 'mix and match' different services into service ensembles. Indeed, in line with its minimum requirements to allow for switching between providers, the DA aims to improve **interoperability for in-parallel use of multiple data processing services with complementary functionalities**. This relates to situations where customers **do not terminate a contractual agreement to switch** to a different provider of data processing services, but where **multiple services of different providers are used in-parallel**, in an interoperable manner, to benefit from **the complementary functionalities** of the different services in the customer's system set-up (Recital 99). The latter could require horizontal interoperability in order to allow a continue exchange of data of complementary services of the same service or at the same level in the vertical value chain in any case.

This setting, according to EU Commission, is aimed to facilitate the successful deployment of **'multi-cloud' strategies**, which allow customers to implement future-proof IT strategies and **decrease dependence on individual providers of data processing services**. Facilitating a multi-cloud approach for customers of data processing services can also contribute to increasing **their digital operational resilience**, as recognised for financial service institutions in the Digital Operational Resilience Act (DORA) (Recital 99).

However, if vertical interoperability plays an important role for service portability and horizontal interoperability could play a role for in-parallel use of complementary services, most of the DPS providers' interactions and switching would probably refer to service of the same service type, perceived as substitutes by users. In this context, a general interoperability obligation may be disproportionate, as interconnection of services of the same service type seems unable to generate additional benefits (further to those granted by one-off data portability obligations). Moreover, an

assessment of technical feasibility as well as the standardisation costs associated with such interoperability obligations should be required in each specific context of consideration.[79]

That said, Article 35, which is explicitly titled "Interoperability for data processing services", seems not to be completely in line with some of the previous provisions and underlying rationales. Article 35.1 describes the functions of open interoperability specifications and harmonised standards referring them to all DPS (comprising IaaS, PaaS, and SaaS). Moreover, it restricts interoperability to services of the same service type. A deeper coordination of this provision with the previous ones seems to be needed.

3.2.8 Enforcement and Institutional governance

The DA is generally enforced at a decentralised level, as Member States must designate one or more National Competent Authorities (NCA) responsible for the regulation application, (Article 37.1) with the restriction that the authority made responsible for the enforcement of switching between data processing services (Chapter VI) and interoperability (Article 35) must have "experience in the field of data and electronic communications services" (Article 37.4(a)). When a Member State designates more than one competent authority, it must also identify among them a "data coordinator" authority responsible to facilitate cooperation between all the different authorities (Article 37.2) and to act as the single point of contact for all issues related to the DA implementation (Article 37.6(a)). In this regard, it is important to underline that Article 37 also establishes a one stop shop mechanism, under which "entities falling within the scope of this Regulation shall be subject to the competence of the Member State where the entity is established." (Article 37.10)

However, the DA explicitly safeguards competent authorities, which would retain responsibilities for the application of the Data Act in their respective areas of competences, namely:

- data protection authorities for matters pertaining to the protection of personal data;
- sectoral authorities for specific sectoral data exchanges;
- authorities with experience in the field of data and electronic communications services for enforcing the provisions on cloud switching (Chapter VI and Article 35 on interoperability for data processing services).

The main competences of the NCAs will be to (a) deal with complaints for alleged DA violations; (b) receiving complaints from stakeholders about DA infringements; (c) pro-actively ensure the compliance of DA provisions regarding switching charges; (d) perform investigations about matters related to DA provisions; (d) impose fines and penalties, as set by national legislation; (d) cooperate with NCAs of the same member State, and of other Member States and with the European Data Innovation Board (EDIB); and (e) cooperate with other sectors/regulation authorities, including the NRA for Electronic communications, and the Data Protection authorities. Each NCA must be able to act independently, both from all market entities and from other public bodies (comprising the national government) (Article 37.8) and must be equipped with adequate human and financial resources (Article 37.9).

[79] Cfr. CERRE (2023) DATA ACT: Towards a Balanced EU Data Regulation

This decentralised and possibly fragmented enforcement system is partially mitigated by some relevant competences allocated to the Commission and by the establishment (or better the empowering) of the European Data Innovation Board (EDIB). Of course, the extensively described formal cooperation duties will also aim to enhance coordination.

As for the EU Commission, under Article 35, it has a primary enforcement role for Article 30.3, which requires DPS providers at the PaaS and SaaS layer to ensure compatibility with open interoperability specifications or European standards for interoperability. To this aim, the Commission can mandate the use of European standards for interoperability or open interoperability specifications for a specific service type (Article 35.8 and Recital 103).

In particular, Articles 35.3 to 35.8 design a pervasive top-down mandatory standardisation process, by empowering the European Commission either (i) to ask standardisation bodies to develop harmonised standards or (ii) to directly adopt implementing acts (also by request of a MS) for common specification based on open interoperability specification publishing the "reference of open interoperability specifications and European standards for the interoperability of data processing services", such that these would become binding interoperability standards in accordance with Article 30.3.

As for the latter, the EDIB is to be set up as a Commission expert group, aimed to assist the Commission in coordinating national practices and policies on the topics covered by the Data Governance Act[80] (DGA) (Article 29 DGA). Besides the representatives of the authorities competent to apply the DGA,[81] the EDIB will also comprise representatives of the DA competent national authorities (DA Article 42).

According to the DGA, in addition to other competences, the EDIB will support cross-sector data use by adhering to the European Interoperability Framework principles and through the use of European and international standards and specifications. Work on technical standardisation could include the identification of priorities for the development of standards and establishing and maintaining a set of technical and legal standards for transmitting data between two processing environments that allows data spaces to be organised, in particular clarifying and distinguishing which standards and practices are cross-sectoral and which are sectoral.

As said, those competences will be supplemented by those foreseen by Article 35 DA regarding DPSs. The DA specifically states that EDIB promotes and supports the regulation's consistent application by: (a) advising the Commission; (b) facilitating the cooperation of NCAs; (c) advising and assisting the Commission with regard to: (i) whether to request the drafting of harmonised standards referred to in Articles 33.4, 35.4 and 36.5;); (ii) the preparation of the implementing acts referred to in Articles 33.5, 35.5, 35.8 and 36.6; (iii) the preparation of the delegated acts referred to in Articles 29.7 and 33.2; and (iv) the adoption of the guidelines laying down interoperable frameworks for common

[80] Regulation (EU) 2022/868 of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act).

[81] The DGA states that other representatives will come from the European Data Protection Board, the European Data Protection Supervisor, the European Union Agency for Cybersecurity (ENISA), the Commission, the EU SME Envoy.

standards and practices for the functioning of common European data spaces referred to in Article 33.11.

3.3 Digital Markets Act

3.3.1 Legislative objectives and structure

The Digital Markets Act sets the **harmonised regulatory framework** for a few digital platform services, aiming to enhance contestability and fairness for final users and business users of those services.[82] The DMA works as a **complement of EU competition law**, which has been considered not sufficient to completely address those problems in digital markets. This is because (i) the scope of Article 102 TFEU is limited to certain instances of market power, and (ii) enforcement occurs ex post and requires an extensive and complex investigation on a case-by-case basis. Moreover, (iii) Core Platform Services (CPSs) are not necessarily a relevant market, in the competition law meaning, and are not necessarily are dominated by one company (Recital 5 DMA).

As for the regulation objective scope, the DMA focuses only on **those digital services considered by co-legislators as the most used by business and end users, defined as 'core', where currently the most concerns about low contestability and unfair practices** (Article 1.2 DMA). Therefore, the DMA's regulatory measures are expressly limited to Core Platform Services (CPSs), listed in the legislation (yet subject to periodic revision).

In those CPSs, large economies of scale, direct and indirect network effects, and data-driven advantages can negatively impact fairness in the commercial relationship between undertakings providing such services and their business users and end users, as well as the contestability and competition dynamics, resulting in lock-in effects and lack of multihoming, both at CPS (upstream) level and in the business users' market, especially when CPS providers are vertically (or horizontally) integrated (Recital 2).

The distinction between end users and business users is crucial in the DMA as the concerns of contestability and unfair practices identified in the legislation arise predominantly in respect of two-sided services constituting an important gateway for business users to reach consumers (Recital 15), such as digital platforms that individually intermediate between business users and end users.

Indeed, the **DMA is an asymmetric regulation**, imposing obligation only on undertakings in respect of CPSs for which they qualify as a '**gatekeeper'** and may therefore be in a position to control or profoundly influence choices and access for a very large number of end users and business users, tending to play the role of a new institutional mechanism with selecting, allocating, and informative functions. [83]

In particular, the DMA defines gatekeeper as an undertaking that provides a CPS in at least three member states and meets three general qualitative criteria (Article 3.1): (a) it has a significant impact on the internal market; (b) it operates a CPS that is an important gateway for business users to reach end users; and (c) it enjoys (or can be expected to enjoy soon) an entrenched and durable economic

[82] In general about the DMA, CERRE (2023) Effective and Proportionate Implementation of the DMA
[83] Cfr. Manganelli A., Nicita A. (2022) Regulating digital markets: the EU Approach

position in its operations. The DMA also identifies quantitative thresholds, by respectively translating and quantifying the qualitative criteria, from which the gatekeeper status is presumed (Article 3.2). This presumption takes place when an undertaking (a) achieves an annual Union turnover equal to or above EUR 7,5 billion in each of the last three financial years, or where its average market capitalisation or its equivalent fair market value amounted to at least EUR 75 billion in the last financial year, and it provides the same core platform service in at least three Member States; (b) it provides a core platform service that in the last financial year has at least 45 million monthly active end users established or located in the Union and at least ten thousands yearly active business users established in the Union, identified and calculated in accordance with the methodology and indicators set out in the Annex; (c) threshold (b) was met in each of the last three financial years.

An essential aspect of the regulation of digital markets is therefore the identification of gatekeepers, an activity entrusted exclusively to the Commission and reviewed at least every three years, including on the basis of the notifications that CPS providers are obliged to make if they reach the quantitative thresholds (Articles 3, 4 and 15).

Gatekeepers are subject to 21 obligations (Articles 5 and 6), whereas undertaking designated as gatekeepers for number-independent interpersonal communications services are formally subject to an additional horizontal interoperability obligation (Article 7). Those obligations aim to generally tackle behaviours that DMA qualifies as “particularly harmful or unfair” if engaged in by gatekeepers. For this reason, all prohibitions are directly applicable ex-ante, without any need for further case-by-case analysis.

Indeed, the rationale of the DMA is to introduce a set of obligations that have a cumulative impact on the contestability and fairness of digital markets whose specific market failures have been assessed and addressed in a systemic, general, and abstract manner, “independently from the actual, potential or presumed effects of the conduct of a given gatekeeper … on competition on a given market.” (Recital 11)

This regulatory architecture and approach has, however, to be interpreted in the light of the asymmetric and horizontal nature of DMA as a pro-competitive regulation. An asymmetric regulation is, by definition, inherently effect-based (at least in its design), since it imposes regulatory obligations only on some stakeholders because of the effects that those companies' unregulated behaviours would (risk to) cause. Yet, the DMA is also a horizontal piece of legislation, since the same provisions (Articles 5 and 6, yet not Article 7) disciplines different ‘core platform services’ operating in different markets (not necessarily an antitrust meaning) and under different business models.

The combination of these two characteristics could prove to be problematic as an ex-ante asymmetric definition of (il)licit behaviours becomes more and more complicated the larger the scope of business models, services, and markets covered by that regulation is. In other words, a complete harmonization of ex-ante remedies across a number of different CPSs and the different entities identified as gatekeepers could prove problematic. Indeed, digital markets are not a sector or an industry.

Usually, horizontal pieces of legislation are tendentially symmetric (such as data protection, or consumer protection), whereas sector-specific pro-competitive regulation could be easily found in an

asymmetric fashion (in the electronic communications regulation where Significant Market Powe (SMP) operators are all quite similar, for instance). The relevant exception (the elephant in the room) in this taxonomy is represented by competition law (namely Article 102 on the abuse of dominant position), which is asymmetric (posing a special responsibility only on dominant players) and horizontally applied to all sectors of the economy. However, competition law is composed of (very few) principle-based provisions, which can be interpreted in an adaptive way with regard to specific market contexts (and in time dynamic way) within a case-by-case enforcement activity. Yet, this possibility was explicitly and intentionally excluded for the DMA in order to ease and speed-up its enforcement.

The effect-based assessment in the DMA design was mainly borrowed from competition case-law in digital markets, so codifying specific interpretations and applications of principle-based competition law provisions, and unavoidably extending their application scope compered to each single competition case. This has raised a number of critiques in relation to the possible inaccuracy or uncertainty implied by applying quite a few detailed obligations to different services, markets and business models (whereas usually ex-ante pro-competitive regulation is sector-specific). [84]

Moreover, it has been noted[85] that the failure to adapt rules to the specific features of each gatekeeper and CPS, coupled with the imposition of many highly detailed obligations, also affects the ability of rules to adapt to changes in the relevant market, which is a feature to be considered extremely relevant in complex and changing industries such as digital ones. As a matter of fact, elements of adaptation of the rules are provided for in the regulation, and those are extremely relevant for its effective and efficient dynamic application.

3.3.2 Cloud Computing Services as CPS

Cloud Computing Services (CCSs) are one of the Core Platforms Services listed in the DMA (Article 2(2)).[86] CCS is defined as: "a digital service that enables access to a scalable and elastic pool of shareable computing resources."[87]

The inclusion of CCSs in the list of CPSs, according to the principle of proportionality, is based on a perception that these services are susceptible to the trends of tipping with an overall lack of contestability as well as lacking fairness in the relationship between gatekeeper, on one side, and end and business users, on the other.

[84] For example, Larouche P, De Streel A. (2021) proposed to design DMA by including a core narrower set of obligations (suitable for all gatekeepers) along with an additional, broadly worded, principle-based closure prohibition, to be applied on a case by case basis. Others, Caffarra C., Scott Morton F. (2021), to design ex-ante rules divided by categories of business models, thus creating differentiated sets of rules for each category.

[85] De Streel A., Larouche P. (2021) The European Digital Markets Act proposal: How to improve a regulatory revolution, Concurrences N° 2-2021, pp. 46-63,

[86] The complete list of CPS is as follows: (a) online intermediation services; (b) online search engines; (c) online social networking services; (d) video-sharing platform services; (e) number-independent interpersonal communications services; (f) operating systems; (g) web browsers; (h) virtual assistants; (i) cloud computing services; (j) online advertising services, including any advertising networks, advertising exchanges and any other advertising intermediation services, provided by an undertaking that provides any of the core platform services listed in points (a) to (i).

[87] Article 2(13), referring to Article 4(19) Directive (EU) 2016/1148.

However, a relevant peculiarity of CCSs is that, unlike other CPSs, they are one-sided rather than two-sided in nature (see **Section 4** for a deeper economic assessment).[88] CCSs do not intermediate between two different groups of customers[89] and do not provide a "gateway for business users to reach end-users" (and the importance of such a gateway represents one of the qualitative features for the definition of a gatekeeper according to Article 3.1 (b)).

In this regard, Recital 2 observes that "characteristics of core platform services are very strong network effects, an ability to connect many business users with many end users through the multisidedness of these services", and consequently **Recital 15** states that "DMA obligations should only apply to undertakings designated as gatekeepers and should only apply to those of their core platform services that individually constitute an important gateway for business users to reach end-users."

One could give a very extensive interpretation of the 'gateway' concept, seeing an upstream infrastructure/service as an "important gateway to reach end-users" for example in a situation where a business user, that is, a downstream provider, could not provide its service without that facility and thus behaves as an access seeker. In any event, a vertical pipeline value chain is something different to a platform value chain and is not compatible with a two-sided market structure.

This could have an impact on (i) the designation of gatekeeper(s) of CCSs; and, above all, (ii) the applicability/relevance to that gatekeeper of some of the obligations under Articles 5 and 6.

This may be different in those circumstances where an **independent software vendor (ISV)** develops IT services and offer them to end-users as SaaS services, via the **marketplace of cloud providers** and built on the IaaS and/or PaaS environment of cloud providers. However, such marketplaces are unlikely to fall within the DMA definition of a CCS and are more likely to be considered an intermediation.

3.3.3 Designation of CCSs as gatekeepers

DMA is an asymmetric regulation which is imposed only to companies designated as gatekeepers under Article 3, with respect only to CPSs they provide that meet the requirements in Article 3.1(b). Designation of a gatekeeper refers to each specific CPS - as well as the quantitative thresholds 3.2(b) and 3.2(c), whereas Article 3.2(a) is referred to companies. Therefore, the gatekeeper status is not attached to a company satisfying all thresholds for one CPS and automatically extended to all other CPS provided by that company.

[88] With the relevant exception of the online messaging services (NI-ICS), which are not two-sided market (even if DMA Recital 15 underlines "the fact that it is possible that an undertaking providing core platform services not only intermediates between business users and end users, but also between end users and end users, for example in the case of number-independent interpersonal communications services, should not preclude the conclusion that such an undertaking is or could be an important gateway for business users to reach end users."). However, CCS neither do intermediate between end users and end users, which is the same as saying that, differently from NI-ICS, CCS do not exhibit direct (same-side) cross externalities. That's why horizontal interoperability obligation for NI-ICS is always pro-competitive (Article 7 DMA), while, as described in the previous section, DA interoperability obligations at horizontal level could give raise to doubts for CCS (unless there are complementary services).

[89] More completely, we consider a two-sided market as composed by two groups of agents who interact via a platform, selling two different products or services to two different groups of customers, considering that demand from at least one group depends on demand from the other group (no externality for the platform), while customers of the two groups do not take these indirect (cross-group) network effects into account.

Articles 3(1) and 3(9) are key to a correct conceptualisation of the gatekeeper designation: that status is attached to a company only with respect to any CPS it provides that is "an important gateway for business users to reach end users" (Article 3.1(b)). A CPS is presumed to satisfy these criteria if it satisfies the quantitative thresholds[90] set out in Article 3(2)(b).

Therefore, the 'important gateway' concept in Article 3(1)(b) and its quantitative translations in Article 3(2)(b) are critical to determining whether a certain CPS falls within scope of the DMA. In this regard, considering the lack of network externalities, on the one hand, the two-sided market structure is not applicable to CCSs and, on the other hand, the economic qualification of companies buying services from gatekeepers could be uncertain. Therefore, defining what is a CCS business user (and an end user) for the application of Article 3 is crucial.

Under Article 2(21) DMA a 'business user' is generally defined as any natural or legal person acting in a commercial or professional capacity using core platform services **for the purpose of** or **in the course of** providing goods or services to end users. This definition outlines a concept of business user broader than the P2B definition - Article 2(1), which explicitly refers to platforms' intermediation services. Indeed, DMA business user can **use CPS in the course of providing its services** to end-users, without necessarily being intermediated via à vis end users, and thus enlarging the possible relationship between gatekeepers and business users.

Therefore, the definition in Article 2(21) can comprise different meanings of what a business user is, that's why there are CPS-specific definitions included in the Annex, which are meant to operationalise the quantitative thresholds. The DMA Annex defines CCS's active business users as "the number of unique business users **who provided any cloud computing services hosted in the cloud infrastructure of the relevant provider of cloud computing services** during the year".

Given the broad definition of 'cloud computing services' in the DMA, there is uncertainty around what these definitions of 'business users' mean in the context of CCSs. One potential interpretation may be that these are users that have a relationship with a gatekeeper similar to what happens in a traditional vertical pipeline value chain. In other words, it may be interpreted to cover users that:

- are not part of a two-sided market relationship;
- provide the same CPS as their gatekeeper, yet at a different level in the vertical value chain;
- act as access-seekers of an essential asset; and,
- are always (potential) competitors of the gatekeeper for the same end-users.

Such a characterisation can lead to a small, yet meaningful, paradox in the DMA enforcement. If CCS business users are access seekers and (potential) competitors for their gatekeeper, depending on the gatekeeper's market share (which is not assessed under DMA), the number of business users could directly reflect the intensity of downstream competition. Therefore, not designating a CCS that has no business users (or a small number of business users which does not meet the threshold) could mean not pro-competitively regulating the companies that possibly have a greater market power, as these

[90] For the sake of simplicity, we do not consider for the moment (a) the possibility of stakeholders to ask for a rebuttal of the presumption when the quantitative thresholds are met and (b) the possibility for the Commission to proceed with the designation when the quantitative threshold are not met.

have smaller downstream competitive pressure. The origination of this paradox is quite understandable considering that DMA has been conceived for two-sided platforms.

As far as 'end users' are concerned, according to the DMA, these are "any natural or legal persons using core platform services other than as a business user". If this definition makes perfect and clear sense for a two-sided market where platforms intermediate between business users and end users , it however creates interpretative uncertainties for CCS.

On the one hand, a strict interpretation can be given to what 'using a CPS' means (as the DMA Annex does), thus considering those end users that are customers of the CPS provider. However, those CPS customers do not necessarily have any relationship with the business users. So, it is difficult to understand how the CCS provider could be an important (or even unimportant) gateway for business users to reach them. The wording of the DMA does not support a more extensive interpretation of the 'end user' concept to encompass also those users indirectly using a CPS via a business user, that is a customer of a business user accessing the CPS in the vertical pipeline model. The DMA Annex defines CCS's active end users as "number of unique end users **who engaged with any cloud computing services from the relevant provider of cloud computing services** at least once in the month, in return for any type of remuneration, regardless of whether this remuneration occurs in the same month." The verb 'to engage' and the clear reference to payment of remuneration by the end user to the gatekeeper indicate that there must be a direct relationship between end users and candidate gatekeeper, thereby excluding the possibility to give an extensive interpretation.

Again, these uncertainties derive from the fact **that CCSs are not two-sided services and thus, in the proper sense, they can't be a gateway for business users to reach end users,** which questions the strong relationship between the quantitative and qualitative thresholds and therefore the robustness of the underlying presumption. Therefore, **it is extremely difficult to find a systemic interpretation of these concepts, which can make the designation of CCS gatekeepers operational and meaningful at the same time**.[91] Nevertheless, **considering the definition of CCS business users and end users, the designation of gatekeepers under Article 3 would not be affected by the described paradoxes and uncertainties if quantitative thresholds are met.**

However, the peculiarities of CCSs **could make it very burdensome for the Commission to designate a CCS provider as gatekeeper, under Article 3.8, using the qualitative characteristic if the presumptive quantitative thresholds are not met.** The criteria to be applied by the Commission are wide ranging, but the gatekeeper must satisfy each of the three qualitative criteria in Article 3.1. Among them, as said, the qualitative concept of important gateway, when deprived of the quantitative operational definition, seems hard to sustain. Moreover, the lack of network externalities, both indirect and direct is also relevant in the same sense among other additional elements to consider.

On the other hand, in case a CCS provider is designated as gatekeeper, another relevant issue, could be whether these peculiarities of CCSs as CPSs **could help to rebut the presumption under Article 3 (5)**. Article 3(5) states that such a rebuttal is an 'exceptional' outcome. However, it is not clear the

[91] Of course, this analysis considers CCS as a stand-alone CPS, while these considerations should be adjusted in the enforcement activity in light of the overall conglomerate ecosystem of each specific gatekeeper.

legal meaning of 'exceptional' and whether the intention is for the same evidential thresholds and relevant factors to apply in both to firms submitting arguments under Article 3(5) and Commission own assessments under Article 3(8).[92]

Finally, it is important to note that no CCS provider has been designated as gatekeeper by the EU commission in the first round of designation in June 2023.

3.3.4 The application of DMA remedies to CCS's gatekeepers

DMA obligations for all gatekeepers are listed in Articles 5 and 6 (while Article 7 defines the interoperability obligation for NI-ICS). Article 5 contains the obligations that do not require additional specifications, whereas obligations in Article 6 may require additional specification by the Commission, under Article 8, in relation to a specific CPS and/or gatekeeper. These obligations only apply in case of gatekeeper designation: as no CCS provider has been designated, we treat them under this section under the purely hypothetical situation.

Because of the peculiar features of CCSs as CPSs, **only a subset of DMA provisions seems to be completely relevant and applicable** for them (in a circumstance in which a CCS provider would be designated as gatekeeper) at a first analysis.

Those provisions are, as for Article 5:

- Article 5(2)(b), (c), and (d), prohibiting the combination or cross-use or cross sign in of end users, unless they give their explicit consent; while Article 5(2)(a) does not seem to be relevant as it refers to an ad-based business model;
- Article 5(6), prohibiting the prevention of end-users to raise issues of non-compliance with public authorities;
- Article 5(7), prohibiting tying of CCSs with ID services, web browser engine or payment services; and
- Article 5(8), prohibiting tying of CCSs with any other CPS.

As for Article 6, they are:

- Article 6(2), prohibiting the use of business users' data in order to compete with them;[93]
- Article 6(5), prohibiting of self-preferencing or discrimination in crawling;
- Article 6(6), prohibiting the restriction of switching or multihoming across services accessed via the gatekeeper service (device neutrality);
- Article 6(9), imposing effective, real-time, and free of charge data portability for end users;
- Article 6(10), imposing real-time, and free of charge data access/portability for business users to data associated with their services; and
- Article 6(13), prohibiting the imposition of disproportionate conditions for termination of services.

[92] Cfr. CERRE (2023) Effective and Proportionate Implementation of the DMA

[93] This provision involves business users, yet Recital 48 explicitly give a specific interpretation of the concept of business users for this obligation extending the obligation: "to data provided or generated by business users of the gatekeeper in the context of their use of the cloud computing service of the gatekeeper, or through its software application store that allows end users of cloud computing services access to software applications";

Other provisions do not seem to be applicable or relevant for CCSs as they refer to **ad-based business model**, such as, Articles 5(2)(a), 5(9), 5(10), or 6(8).

For others their application or relevance for CCSs is unclear as they refer to specific CPSs or subsets of all CPS not clearly including CCS. Those are:

- Article 6(3), enabling to uninstall apps on Operating System and allow easy changing of settings on Operating System, virtual assistant, or browser;
- Article 6(4), allowing side-loading and vertical interoperability for third-party apps and app stores;
- Article 6(7), allowing access and vertical interoperability for providers of services or hardware to the same features of Operating System, or virtual assistant;
- Article 6(11) data sharing for search engines about ranking, query and clicks; and
- Article 6(12) access for business users to app stores, search engine and social network at FRAND.

All of them are obligations susceptible of further specifications under Article 8, which could be necessary for CCSs if designated.

Finally, there is a group of provisions that refer to business users and to the intermediation function of the gatekeepers. Considering the untrivial definition and conceptualisation of business users for CCSs, it appears interesting to have some further reflection on them. Those provisions are:

- Article 5(3), prohibiting MFN-like and parity clauses;
- Article 5(4), prohibiting anti-steering and allowing business users to communicate with end users off platforms; and
- Article 5(5), prohibiting anti-disintermediation actions, thus allowing end users to access and use services even if acquired elsewhere.

In particular, Article 5(3) states that "the gatekeeper shall not prevent **business users** from offering the same products or services to end users through **third-party online intermediation services** or through **their own direct online sales channel** at prices or conditions that are **different from those offered through the online intermediation services of the gatekeeper**". Here, the specific and enlarged definition of CCS business should be reconducted to the general one applicable for two-sided markets, as the provision makes explicit reference to the intermediation service of the gatekeeper. Therefore, this provision seems to be applicable only for IVSs and Cloud marketplaces.

Within a cloud marketplace model, the marketplace provider's services and business users' ones are still (potentially) the same. This is exactly what happens also for the general commercial marketplace (where a marketplace provider can work both as an intermediary and also as a retailer), yet for general commercial marketplaces the vertical integration is limited to intermediation and 'downstream' services (or better retail services as there is a platform structure). Whereas for CCSs, vertical integration could combine the platform model integration, that is, intermediation services, with the pipeline model vertical integration between a proper upstream and a proper downstream service.

Therefore, an alternative intermediary must be either (a) vertically integrated too, possibly the business user itself, or (b) in need to access the upstream service of the gatekeeper. The first

occurrence seems somehow to be covered by Article 5(4), which imposes to the gatekeeper to "**allow business users**, free of charge, to communicate and promote offers, including under different conditions, to end users acquired via its core platform service or through other channels, and **to conclude contracts with those end users**, **regardless of whether, for that purpose, they use the core platform services of the gatekeeper**."

The second option is covered by Article 5(5), which imposes gatekeepers to "**allow end users to access and use, through its core platform services, content, subscriptions, features or other items, by using the software application of a business user**, **including where those end users acquired such items from the relevant business user without using the core platform services of the gatekeeper**." This last provision applied in a vertical pipeline value chain could be reminiscent of a consumer-led access obligation imposed on upstream CCS providers, if designated as gatekeepers. The regulatory and economic meaningfulness of such a provision is not trivial.

However, as previously mentioned, in a cloud marketplace scenario, a marketplace service (which intermediates CCSs) would likely be considered a separate, yet interrelated service, from CCSs and, if the threshold was met, be designated as a gatekeeper for Online Intermediation Services. Of course, for a vertically separated situation (that is, a cloud marketplace service provider not supplying CCSs) the situation appears significantly clearer (which by the way seems the scenario that EU commission envisages in its data strategy). Yet, this does not look like what the industry could reach autonomously.

In conclusion, considering the peculiarities of CCSs as CPSs, additional specifications for Article 6 obligations under Article 8, as mentioned, could prove very important for CCSs, as well as a possible extensive interpretation of Article 8 itself, related to the potential formal applicability to CCS gatekeepers of a meaningful subset of all the provisions, as described.

The last point is also related to an application of the proportionality principle to the DMA, which is a general EU law principle, especially when it comes to economic regulation. As mentioned, proportionality is a general principle of EU law, under Article 5(4) TEU[94], which applies at macro level for the definition of the scope of regulation (in the law-making process) and in the DMA contributed to limit obligations to certain services that are problematic in terms of fairness and contestability. This principle always applies at micro level as well, in the enforcement activity, for instance (which is a substantive part of the 'union action').

In particular, it means that applied regulation, that is, the actual restriction of stakeholders' licit behaviours, should be such to effectively address the problem at stake while imposing the smallest restriction possible on market players' freedom. It does not seem plausible that such a complex assessment was completely performed by the legislator in the law-making process, especially considering the number of different services, markets and business models involved, as well as the specific peculiarities of CCSs among the other CPSs.

[94] "Under the principle of proportionality, the content and form of Union action shall not exceed what is necessary to achieve the objectives of the Treaties".

Moreover, for ex-ante pro-competitive regulation this acquires a specific meaning related to the relationship with competition law. The complementarity of the two, explicitly stated by the DMA (Recital 10) (yet also unavoidably enshrined in the EU legal structure, under which competition law is primary law while all regulations are secondary law) is also based on a proportional application of ex-ante regulation. Indeed, the minimum effective restriction of stakeholders' behaviours on the one hand try to preserve decentralised market dynamics (and its efficiencies) and minimise regulatory failures due to information asymmetry as much as possible; and on the other hand, the residual freedom left to the regulated company is always (if and where gatekeepers are dominant players) subject to competition law, which could, when necessary, restrict further the licit behaviours (especially when regulation does not restrict sufficiently the set of licit behaviours).[95]

Therefore, antitrust intervention in regulated markets does not represent a regulatory failure, but represents one side of a two-sided institutional enforcement mechanism in which ex-ante regulation represents a complement to it. In a dynamic fashion, this complementarity is also able to guide the revision of the regulation, either enlarging its scope or reducing it. This is even more true when regulation and competition law enforcement are allocated to the same body, thus internalising any possible coordination cost and institutional externality.

3.3.5 Enforcement and institutional governance

From an institutional perspective, the DMA is marked by strong centralisation. In fact, the primary rationale for the regulatory framework, stemming from both the regulatory basis for harmonisation of national regulations (Article 114 TFUE) and the choice of the directly applicable regulatory instrument of regulation (instead of directive), is in fact to avoid national fragmentation of both rules and their implementation.

From a substantive point of view, the centralised set-up of the DMA is in the first instance justified by the global nature of the regulated entities, which, on the one hand, requires greater harmonisation and consistency of application and, on the other hand, leads to a greater effectiveness of rules if applied by an entity capable of supervising a greater number of markets and users.

From an opportunity-cost analysis perspective, the centralisation of enforcement entails the elimination (or reduction) of negative externalities arising from the uncoordinated interaction of various decentralised actors. Namely, (a) the possible duplication of enforcement costs in case several authorities intervene on the same case; (b) the legal uncertainty associated with the possibility that similar cases may be treated differently in different member states; and (c) possible external effects (positive or negative) arising from the action of one authority that are not taken into account by other authorities. While the benefits generally associated with a decentralisation choice, namely (i) reduction of the Commission's workload so that it can select cases and focus on the most relevant ones, and (ii) benefits in terms of effective use of dispersed information, seem in this context to be

[95] This dynamic also results in a risk (cost) re-allocation in relation to the information asymmetry: from the social dimension to the dominant regulated company, entailing a specific further responsibility based on the combination of antitrust and sectoral provisions. Namely, the regulated company, besides what stated in the regulatory provision, has the responsibility to pro-actively cooperate (primarily by providing adequate and truthful information) with regulators in order to define efficient and effective pro-competitive rules. If it fails to do so, and regulator defines a suboptimal set of rules, this could represent an abuse.

smaller than those arising from centralisation. In fact, both of these advantages are marginal because of the small number of gatekeepers, on the one hand, and their global size and nature, on the other.

This pronounced enforcement centralisation clearly differentiates the DMA from all the other existing ex-ante pro-competitive regulatory frameworks. For example, within the electronic communications framework, pro-competitive regulation, although subject to binding vertical and horizontal mechanisms of harmonisation and coordination, is decentralised to the national level to allow regulators to tailor, to some extent, the application of rules to national market circumstances and operators, having a national dimension. This tailoring activity on a national base is definitely not necessary for gatekeepers because, as pointed out, although they could differ from one another in different CPSs, each one operates in all member states and does not differentiate its business and market strategies geographically (except in response to different national regulation).

The centralised set up of the DMA also differs from the institutional set up of competition law, where, under the Modernisation Regulation, a decentralisation implementation is defined. However, the empowerment of national competition authorities (the modernisation) came after decades of centralised implementation, which built a consolidated case-law by the Commission and European courts giving a clear guidance to decentralised enforcers. Moreover, under the Modernisation Regulation, decentralised enforcement of European competition law is mitigated by a role of functional primacy that the European Commission has maintained, primarily through Articles 11.6 and 16.2 of Regulation 1/2003. Finally, in this context of complementarity between regulation of gatekeeper and competition law, the Commission's role of functional primacy in the enforcement of EU competition law – and especially its exercise in practice, including through Article 11(6) – seems even more crucial in order to avoid a stratification of enforcement interventions of the two sets of rules by different actors.

3.4 Interactions between Different Pieces of EU Legislation

3.4.1 Introduction

Data is a crucial resource for the overall digital economy and consequently quite a few pieces of legislation within the EU data strategy have been issued. These have different objectives and rationales, and cover different data targets (see table on the next page).

Piece of legislation	Year of adoption	Objectives	Kind of data covered
GDPR	2016	(a) Ensure high-level of data protection; and (b) free flow of personal data.	Personal data
Free Flow of Data	2018	Ensure free flow of data other than personal data	Non-personal data
Open Data Directive	2019	Promote the use of open data and stimulate innovation in products and services by governing the re-use of public sector and publicly funded information	Data in open format
Data Governance Act	2022	(a) Re-use of certain categories of data held by public sector bodies; (b) framework for the provision of data intermediation services, in order to ensure trust for data transaction; and (c) voluntary registration of entities which collect and process data made available for altruistic purposes.	(a) Non-personal and anonymised personal data held by public sector (b + c) non-personal and personal data made voluntarily available by data holders
Digital Markets Act	2022	Contribute to the proper functioning of the internal market by ensuring for all businesses contestable and fair markets in the digital sector where gatekeepers are present, to the benefit of business users and end users.	Personal and non-personal data gathered by gatekeepers either from end-users or business users
Data Act	2023	(a) Making product data and related service data to the user of the connected product or related service; (b) making data by data holders available to data recipients; (c) making data by data holders available to public sector bodies when there is an exceptional need for that data for the performance of a specific task carried out in the public interest; (d) facilitating switching between data processing services; (e) introducing safeguards against unlawful third-party access to non-personal data; and (f) developing interoperability standards for data to be accessed, transferred and used.	(a+b) personal and non-personal data co-generated by connected products and related services (IoT) (c) private sectors data, which are exceptionally needed by EU public sector to carry out statutory duties in the public interest (personal and non-personal are treated differently), (d+ e + f) any data (personal and non-personal) and services processed by providers of data processing services

Not all those pieces of legislation and not every part of each piece are relevant for Cloud Computing regulation, whereas some of them are crucial and often their interplay is not so easy to interpret, also worth considering the different timing of adoption.

EU legislation and policies about cloud services comprise a number of different pieces of legislation and actions, covering technological, economic, and legal aspects, and aiming at different kinds of results in terms of competition, competitiveness, and consumer protection. Coherence and cross-consistency of all regulations, passing from a clear and consolidated definition of the main legal concepts involved as well as their respective scopes of application and their possible interplays, should

be a primary objective both when conceiving the substantial rules and when drafting the legal documents.

The first crucial interplay is the dynamic interaction between the Free Flow of Non-Personal Data Regulation and the Data Act regarding the switching of cloud computing services. The interplay between these acts have been already examined by explaining the rationale for the Data Act.

A more general and crucial interaction is the one between the Data Act and the DMA, which will be described in the section 3.4.2. Finally, a 'horizontal' interplay takes place regarding how 'data portability' is disciplined within the DMA, the DA, and the GDPR, which will be covered by section 3.4.3.

3.4.2 Interplay between DMA and DA: general issues

Both the DMA (Recital 12) and the Data Act (Article 1.3) explicitly safeguard the application of GDPR provisions. Therefore, DMA and Data Act provisions need to be interpreted consistently with GDPR. Moreover, although GDPR has pro-competitive objectives, the overall objectives of GDPR, on one the one hand, and DMA and DA, on the other, are different and therefore no derogation of GDPR could derive from application of DMA and DA. Also, the objective scopes of application differ, as GDPR refers exclusively to personal data, whereas both DMA and DA apply to both personal and non-personal data.

However, the direct general relationship between the DMA and the DA is more uncertain, as there are no explicit reciprocal safeguards. Moreover, the objectives of the DMA and the DA can substantially overlap, with the DMA aiming to get fairness and contestability for CCSs and the DA (Chapters VI and VIII) aiming to enhance competition and lower barriers to entry. Therefore, both of them introduce measures aimed to empower consumers and reduce lock-in and switching barriers and costs.

Moreover, if the DA (as far as its Chapters VI and VIII are concerned) can be seen as a sector-specific legislation, it could in theory work as a *lex specialis* and derogate some of the DMA provisions (if and where there are normative antinomies),[96] although that remains difficult to reconcile with the fact that the DA is symmetric regulation which in theory should be less prescriptive than the asymmetric DMA. Potentially, when a DMA provision is principle-based and/or the application to CCSs (as a peculiar CPS) may require an adaptive interpretation, the DA provisions may be interpreted as a minimum benchmark.

For example, this could be the case in relation to service termination, namely Article 6(13) DMA, on the one side, and Articles 23, 25, 29 DA, on the other. Besides the usual difference in the scope of application of the different provisions, the DMA rule is principle-based, whereas the provisions in the DA about termination of contract and service are extensively detailed and thus could provide the enforcement interpretation baseline for the DMA.

[96] In case of relevant antinomies, another aspect to consider is that DA is passed later than the DMA, so it might implicitly amend it.

Generally speaking, in a normal regulatory setting, an asymmetric regulation builds on the symmetric rules and supplement them for certain stakeholders by adding further obligations. However, as discussed, this could only be partially true in the DMA – DA relationship. The DA (Chapters VI and VIII) is composed of rules intensively constraining DPS providers' behaviours, as far as switching and interoperability are concerned. Those are likely stricter than the DMA's rules, since DA aims to shape the market structure according to a specific vision (that is, a seamless multi-vendor and interoperable cloud environment), thus profoundly influencing and guiding all market players' behaviours and strategies. Nevertheless, the DMA defines additional provisions, only for few companies, to reduce barriers to entry, facilitate porting of data and switching/combining of cloud services.

Therefore, the need to establish a proper relationship between the DMA and DA could be very variable, creating high uncertainty. Unfortunately, this outcome could be magnified by the different enforcement design and authorities called to apply those two pieces of legislation. Indeed, DMA is characterised by a centralisation of the enforcement, whereas the DA is decentralised and potentially fragmented also at national level.

A DA decentralised enforcement could be justified by the fact that the DA, as a symmetric regulation, targets also entities that could have a national dimension, however considering the preeminent objective to create an EU interoperable and single market for data, the consolidation and harmonisation aspects are crucial in any case. Moreover, as previously noticed, the striking asymmetric institutional design vis à vis the DMA could result in a problematic lack of coordination between the two pieces of legislation. That's why the EDIB role at EU level becomes extremely important in order to avoid an inconsistent implementation of the law and market uncertainty. This is of course much easier if there is a centralised enforcement, yet also a decentralised enforcement with strong formal coordination mechanisms (as it is the case for telecom NRAs, BEREC, and the European Commission for example) could result in a similar outcome.

On the other side, an excessive fragmentation at national level could represent a risk deriving from incoherent applications and institutional externalities. Indeed, having more than one authority involved in the same regulatory process, if coordination is effective and incentives aligned, could bring a broader expertise from various sectors, however this inevitably increases those risks. In the institutional setting defined by the DA this risk appears quite a tangible because of both the possible designation of multiple national competent authorities and the retention of competences by existing authorities (that is, data protection and electronic communications NRA). In such a case, an important coordination role is played by national data coordinator. Nevertheless, EU legislations should facilitate their mission by setting some constraints to an excessive fragmentation, by, for instance, allocating new competences defined by the DA to already existing national authorities (as defined in previous EU legislation). This would not go against the principle that each Member State is competent to identify and designate national enforcers, as the EU rules would only identify bundles of competences (defined in different normative acts) allocated to the same body, in an abstract manner, which will be identified concretely by each member state.

3.4.3 Data portability and interoperability for CCS under combined provisions

Data portability (DP), as seen, is crucial to the free flow of data and also as a pro-competitive remedy to unlock a market where data are crucial, in particular for CCS services. DP for CCSs is disciplined by the three main pieces of legislation examined: GDPR, DMA and Data Act, yet in different ways, depending on the different features, objectives and scopes of these legislations. The interplay between each pair of them is not trivial, least of all the interplay among all of them.

As for the GDPR - DMA relationship, despite the European legislature's stated intention that the DMA should "apply without prejudice to the rules resulting from other acts of Union law regulating certain aspects of the provision of services covered by this Regulation, in particular Regulations (EU) 2016/679" (DMA Recital 12), some of the DMA's provisions concerning the processing of personal data could generate the need of coordination with Article 20 of the GDPR.

Indeed, Article 6.9 of the DMA imposes an obligation on gatekeepers to ensure the effective portability of data generated by user activity. Like GDPR data portability, this DMA provision aims not only to ensure that the end user can access and view his or her personal data collected by the platform, but also aims to give the ability to have this information transferred to third-party operators. The underlying goal is of course to reduce the lock-in effect that routinely occurs to the detriment of users confined within each digital ecosystem. The DMA is of course much more explicit than the GDPR in stating that data portability is primarily aimed to “ensure that gatekeepers do not undermine the contestability of core platform services, or the innovation potential of the dynamic digital sector, by restricting switching or multi-homing, end users, as well as third parties authorised by an end user." (Recital 59)

In order to frame the relationship between the portability regimes under the GDPR and the DMA, it is appropriate to compare both with respect to the respective scope as well as with respect to the underlying assumptions of the two bodies of legislation. Regarding the scope of application, the GDPR refers only to the processing of personal data, while the DMA may refer more generally to all types of data that are provided by an end user. For some CPSs this feature would probably apply only/mostly to personal data, however for CCSs it seems to be applicable to both personal and non-personal data. Moreover, considering the non-trivial distinction between personal and non-personal data in the digital environment, the larger DMA scope would also contribute to minimise uncertainty and litigation. Indeed, in light of the contestability objective, it would not make much sense to distinguish between personal and non-personal data, as either of them represents a valuable and competitive asset in digital markets. Consistently, the scope of the DMA further oversteps the GDPR’s by including data not provided directly by data subjects, that is, inferred data or data anyway “generated through the activity of the end user in the context of the use of the relevant core platform service the result of further analysis based on personal data”.

The greater objective application scope of the DMA is combined with a smaller subjective scope, due to the asymmetric nature of all DMA obligations as opposed to the symmetric nature and comprehensive application of Article 20 GDPR. Both these differences could be the result of the overall different policy objectives of GDPR and DMA when considered as a whole, that is, the protection of individual rights, on the one hand, and the protection of competitive dynamics and market

contestability, on the other. In view of this, it has been argued that the two instruments give rise, with reference to data portability, to two parallel instruments of data governance.[97] However, this reading does not seem completely convincing, as those differences could be the result of a stricter (yet not inconsistent) application of GDPR Article 20 for the few gatekeepers regulated under the DMA, for which other data-related obligation apply.

Firstly, the complexity of the digital environment and of the related legislation push toward an interpretation of the rules in a systemic and coordinated fashion. Secondly, as previously said, when looking specifically at Articles 6.9 DMA and 20 GDPR one can easily identify an underlying affinity in the objectives and regulatory modes of the different provisions, which are in fact aimed at fostering contestability in digital markets and greater fairness in relationships within the data value chain, respecting the individual rights and autonomy of the individuals concerned, who remain free to give or not to give consent to the processing of their personal data.

Therefore, the legislature's intention is to complement and supplement the right to data portability introduced by the GDPR rather than to give rise to a parallel and alternative legal instrument, as explicitly stated (Recital 59). Moreover, this setting is completely in line with the Commission's intentions, as it repeatedly observed the incomplete exploitation of the full pro-competitive potential of the data portability regime defined by the GDPR.[98]

Indeed, as far as the technical implementation of interoperability is concerned, the DMA benefits from the significant experience in data governance accumulated over five years after the GDPR approval, which made EU institutions more aware of the technical obstacles to data sharing. In fact, the right to data portability outlined in the GDPR has many critical issues, which made it particularly challenging to ensure an effective implementation. Indeed, Article 20.1 of the GDPR does not provide detailed guidance on how to ensure and coordinate portability mechanisms between different private and public entities. The DMA, instead, requires the gatekeeper to offer free technical tools to facilitate the effective exercise of data portability, going so far as to recommend the use of "high-quality application programming interfaces" (APIs) (Recital 59).

Notwithstanding the asymmetric nature of the DMA, applying to few companies, the DMA is in fact clearly intended to improve the overall functioning of the GDPR's data portability mechanism. By providing a more detailed regulatory framework to certain safeguards that have proven to be poorly effective, DMA enforcement can work as an indirect benchmark to consolidate the guarantees provided by the GDPR, especially considering its centralised enforcement which prevents possible inconsistent implementation at the level of member states.

That said, however, some stricter features of Article 6.9, which evidently rely on the asymmetric nature of the DMA and pose some asymmetric burdens on regulated entities, are to be applied only to gatekeepers. This is particularly evident for portability that, under the DMA, has to be performed

[97] K. BANIA, T. KARANIKIOTI, D. GERADIN, The interplay between the Digital Markets Act and the General Data Protection Regulation, available at https://ssrn.com/abstract=4203907.

[98] EU Commission (2020), Communication to the European Parliament and the Council, "Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation, COM (2020) 264 final, pages 8-9.

with no costs for the end-users and the recipient, whereas GDPR Article 12.5(c) allows data holders the option of charging a reasonable fee taking into account the costs incurred.

The data portability provision in the Data Act applies symmetrically (like the GDPR), yet it is sector-specific and therefore even more detailed than DMA's portability provision. Indeed, the DA portability obligations are specifically functional to allow switching between providers and are accompanied by a set of provisions regarding information disclosure and other obligations aimed to remove switching obstacles. Next to switching, the DA envisions a **multi-cloud environment for in-parallel use of multiple DPS with complementary functionalities**, extending the data portability concept to interoperability obligations. Such interoperability remedies are not part of the data portability in DMA Article 6.9. As described, in the DMA there are interoperability remedies, yet they are limited to NI-ICS in Article 7, as far as horizontal interoperability is concerned, while vertical interoperability obligations in DMA Articles 6.4 and 6.7 refer quite explicitly to a subset of CPSs. Therefore, obligations under the DA about unbundling and service portability seem not to have substantial interaction with DMA provisions.

The symmetric extension of the data portability obligations in the DA (compared to the DMA) is explicitly justified by a lock-in effect in DPSs that reach beyond gatekeepers, "particularly in PaaS and SaaS cloud markets where interoperability problems are gravest and where hyperscalers have a smaller share of the market".[99] Therefore, the Data Act would present a complementary set of minimum framework conditions to enable switching, which would preserve the asymmetric approach of the DMA versus gatekeepers.

Besides data portability related to switching, the Data Act imposes portability obligations also in relation to data generated by the use of a product or related service, guaranteeing users the right to timely access the data generated and also to make them available to third parties (DA Articles 3, 4, and 5, Chapter II). Here, the DA explicitly extends the right to data portability under Article 20 of the GDPR, which applies regardless of the nature of the data, personal or non-personal, the distinction between actively provided or passively observed data, and the legal basis of the processing under GDPR.[100] These provisions are not referred directly to CCSs, unless a CCS works as a related service of an IoT product, which currently seems to be a residual scenario, yet it could evolve.

In any event, it is interesting to note how these DA provisions are along the same lines as the competition policy objectives defined in the Digital Markets Act. Indeed, in facilitating access to and use of data by consumers and businesses, the Commission does not want to provide regulatory tools that would strengthen the dynamics of data accumulation for large digital platforms. For this reason, Article 5.2 of the DA stipulates that a company that provides Core Platform Services (CPSs) and has been designated as a gatekeeper under the Digital Market Act cannot request or obtain, based on the provisions of the Data Act, access to user data generated by the use of a related product or service. So, the policy objective of the DMA, which is to limit the ability of gatekeepers to combine and exploit data from large numbers of data holders to undermine contestability and fairness in core platform

[99] DA impact assessment

[100] It is noteworthy, however, that the Data Act does not create a legal basis under the GDPR for a data owner to provide access to personal data or make it available to third parties at the request of a user who is not the data subject. (Articles 4.5 and 5.6)

services is reflected in the Data Act by ensuring that the increased data supply primarily benefits users and smaller economic players.

3.5 NIS Directives and ENISA Security Certification Scheme

Next to the free movement of data and the enhancement of market contestability and fairness, another pillar of the EU data strategy is to strengthen the security of data as well as software and hardware infrastructures storying, carrying, and using that data. At the end of 2020, the EC presented an update of the EU Cybersecurity Strategy, which focuses on building collective capabilities to respond to major cyberattacks and establishing effective cooperative conditions among partners around the world to ensure international security and stability in cyberspace.

The EU developed its first cybersecurity regulation in 2016 by adopting the Directive on the security of network and information systems (NIS Directive)[101], which has been recently repealed and replaced by the revised NIS directive (NIS2) that entered into force in January 2023.[102] The first NIS directive also established the European Union Agency for Network and Information Security (ENISA), whose powers and competences were reinforced in 2019 by the Cybersecurity Act (CA).[103] The CA also defined a framework for the establishment of European cybersecurity certification schemes and the European Cybersecurity Certification Group.

The NIS2 Directive aims to enhance safety for digital networks and information, requiring all 'essential' and 'important' entities (that is, entities within certain critical sectors or providing key services such as energy, banking, food productions, and so on which generally meet certain size and capitalisation requirements) to adopt specific cybersecurity measures, by complying with a harmonised set of security and risk-management obligations and reporting rules for cybersecurity incidents. Essential entities are subject to heightened ex ante supervision.

NIS2 enforcement is decentralised, and competences have been assigned to the national competent authorities, which are in turn subject to common supervisory and enforcement measures in order to reduce application inconsistencies across the EU and enhance collaboration among member states, especially in the event of cross-border cybersecurity issues. However pursuant to the 'one-stop-shop' mechanism, sectors that by their nature provide cross-border services and operations, such as cloud computing service providers, will only be subject to the jurisdiction of the Member State their main establishment in the EU is located in. The NIS2 Directive covers a broad range of key sectors, distinguishing between sectors of high criticality and other critical sectors.

Digital infrastructures are considered a sector of high criticality, and cloud computing service providers, when of medium or large size, are classified as essential entities (NIS2 Annex I). Therefore, Cloud service providers are subject to the harmonised cybersecurity regulatory obligations.

[101] EU Directive 2016/1148 on security of network and information systems (NIS Directive).
[102] EU Directive 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)
[103] EU Regulation 2019/881 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology, cybersecurity certification. Repealing regulation EU N 56/2013—Cybersecurity Act

Additional specific substantial requirements in terms of cybersecurity for cloud service providers may derive from an EU Certification scheme that ENISA can propose, and ultimately the Commission can adopt via a delegated Act under Article 49 of the Cybersecurity Act. All the Certification Schemes must satisfy the requirements set out in Articles 51, 52 and 54 of the CA, focusing on (a) a set of security requirements and (b) a range of assurance levels (at least three, that is, 'basic', 'substantial' and 'high'), which represent the confidence that a service meets the scheme's requirements and reflects the level of scrutiny to which the service is subject.

As a matter of fact, following a request from the Commission under Article 48.2 of the CA, ENISA set up an Ad Hoc Working Group for drafting a scheme on cloud services, as part of the European Cybersecurity Certification Framework. To this aim, ENISA launched a public consultation in December 2020, ending in February 2021, and resulting in a first draft of the European Cybersecurity Certification Scheme for Cloud Services (EUCS). This draft EUCS defined:

- A transition path from national schemes in the EU, whose certifications remain valid until expiration, aiming to boost trust in cloud services by defining a reference set of security requirements, including transparency requirements such as the location of data processing and storage;
- a voluntary scheme applicable across the EU Member States, for all kinds of cloud services – from infrastructure to applications – covering three assurance levels:

    1. 'Basic', (designed for non-critical data services and systems), which covers the known basic risks of incidents and cyberattacks;

    2. 'Substantial' (designed for business critical data and systems), which covers known cybersecurity risks, and the risk of incidents and cyberattacks carried out by actors with limited skills and resources; and

    3. 'High'(designed for mission-critical, confidential and sensitive, data and systems, that is, essential to operational continuity), which covers the risk of state of the art cyberattacks carried out by actors with significant skills and resources;

- a compulsory third-party revision system, differently from what is provided in the CA which allows self-certification for basic assurance level;
- a maximum three-year duration for each certification, which has to be reviewed annually, and can be finally renewed.

Within the EUCS amendment process, in August 2023 ENISA issued an updated draft candidate EUCS creating a new level 4 assurance and including new requirements relating to the independence of cloud service providers from non-EU law and that cloud service providers must be headquartered in the EU and not be controlled, directly or indirectly, by any entity having its headquarters outside the EU (so-called "**sovereignty requirement**"[104]).

[104] As defined in a letter sent on 25 May 2023 from a number of US cloud industry associations to Secretaries of U.S. Department of State, Secretary of U.S. department of Commerce and U.S. Trade Representative U.S. Trade Representative

In particular **Annex I** of the last draft EUCS (titled "Protection of European data against unlawful access") sets out the requirements for level 4 assurance certification (which, as described in Chapter 5 of the EUCS, would apply to "the most sensitive cloud services, and more specifically, those that process data, whether personal or not, of particular sensitivity, and the breach of which is likely to result in a breach of public order, public safety, human life or health, or the protection of intellectual property").

The objective of level 4 specific requirements is to prevent and limit possible interference from states outside of the EU with the operation of certified cloud services. Technical measures considered to mitigate this general risk are:

- Cloud service provider storing and processing users' data in the EU;
- cloud service provider may access users' data only under the control of employees who have undergone a specific screening and are located in the EU; and
- any access to a functional component of the Cloud service provider's infrastructure by a supplier, typically for support purposes, must be performed under the control of employees who have undergone a specific screening, and are located in the EU.

Furthermore, in order to mitigate the risk related to the extra-territorial application of third country laws that may interfere or conflict with Union Law or with the national law of the relevant Member State, additional requirements have been included:

- Contracts for certified cloud computing services are governed by the law of a Member State and stipulate that only EU courts, EU tribunals, or EU arbitration bodies to have jurisdiction over disputes related to the contracts;
- certified cloud computing services are operated only by companies based in the EU, with no entity from outside the EU having effective control over the cloud service provider;
- cloud service providers must include the risks related to non-EU laws with extra-territorial application in their global risk assessment and inform their customers about this residual risk, so they can perform their own risk assessment; and
- the cloud service provider's headquarters must be in an EU member state and no undertaking with headquarters outside the EU may control, directly or indirectly, the cloud service provider.

EUCS is a voluntary scheme, as stated by **Articles 48.2 and 56.2 of the Cybersecurity Act (CA)**, which however safeguards the possibility that other EU legislation could specify otherwise and define them binding for specific reasons. Indeed, in the same CA, **Article 56** allows the Commission, via delegated act, to make a specific certification scheme mandatory when, after one of its periodic assessments of the effective use of the certification schemes, it is of the opinion that a mandatory scheme would be necessary to ensure an adequate level of cybersecurity.

Moreover, **Article 21 of theNIS2 Directive** requires Member States and the European Commission to consider relevant European standards when putting into place technical, operational, organisational, and methodological risk-management requirements for essential and important entities.

Finally, even if this goes beyond the scope of this report, in this context, it seems that the inclusion of non-technical requirements as described above in the EUCS has not been assessed against the

objectives and effects of **Article 32 (Chapter VII) of the Data Act**,[105] which aims to put in place safeguards against unlawful international governmental access and transfer of non-personal data. Indeed, Article 32 generally states that "providers of data processing services shall take all adequate technical, organisational and legal measures, including contracts, in order to prevent international and third-country governmental access and transfer of non-personal data held in the Union where such transfer or access would create a conflict with Union law or with the national law of the relevant Member State".

In any event, however, **these non-technical requirements in the EUCS, even in the absence of a mandatory certification, could alter the level playing field between EU and non-EU companies, especially, yet non-exclusively, in relation to public procurement, and ultimately put at risk the access of non-EU companies to substantial parts of EU cloud market.** Noncompliance with level 4 assurance could result in extensive ineligibility for public procurement tenders, as it could be expected that public bodies would (be mandated by law to) include in the procurement and tender specifications the highest level of cybersecurity assurance**.**

Moreover, it is also worth considering **whether and how such level 4 security requirements could be neutralised by or, on the contrary, impede the application of data-related regulatory provisions included in the Data Act, the Digital Markets Act, as well as the Data Governance Act**. For example, may such a design of the EUCS allow a cloud provider to object to interoperability obligations on the grounds that these do not allow it to reach level 4 requirements, and thus undermine security? Otherwise, could the interoperability and data portability obligations (hard law) represent an implicit limit/derogation to implement level 4 requirements, if those remain within a voluntary scheme? Answering these questions is not trivial, and therefore it calls for further caution.

Generally speaking, cybersecurity legislation is not aimed at having a direct impact on competition, contestability, or market fairness, even though it can indirectly empower customers, especially those ones not having such a sophisticated understanding or complete information about the services offered. Setting some minimum qualitative standards (that is, excluding from the market certain low-quality services and products) can generally enhance competition on the merits, minimising companies' strategic and opportunistic behaviours.

Alongside this positive effect, however, cybersecurity legislation may have a direct negative impact on competition whether and where it defines minimum standards that are not correlated to the quality of service, but to companies' features related to nationality, for example. **These kinds of geopolitical non-technical requirements and limitations might be explainable and/or justified from a political standpoint, yet, in any case, they should be clearly differentiated and separated from any economic and technical motivation and assessment**.

Indeed, the Data Strategy wants to ensure trust in technology to realise the full potential of the single market while allowing Europe to lead internationally. It would be therefore important for EU legislations to rely on common elements that would define the components of trust in technologies

[105] Proposal for a Regulation on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017 /2394 and Directive (EU) 2020/1828.

in a way that would be valuable for the single market and the relation between the EU and like-minded countries, in order to identify and agree on elements of cyber governance that characterise 'digital trust' and enable cross-border, trust-based data flows.

3.6 Main Actions on Contestability at the National Level

In addition to the EU legislative initiatives, due to the current and prospective relevance of the sector, a few national authorities have started to look into cloud computing services and their functioning in order to understand whether there are market failures and substantial impediments to the development of an effective competition. In particular, market studies have been carried out by (i) Autoriteit Consument & Markt (ACM), the Dutch convergent regulator (for telecommunications, energy, transport, healthcare and postal services) as well as competition authority; (ii) Autorité de la concurrence, the French National Competition Authority; and (iii) the Office of Communications (Ofcom), the UK regulator of communications and media services, which has also concurrent competition powers to deal with anticompetitive behaviour in broadcasting, spectrum, and telecommunications. In this paragraph a brief general description and contextualisation of these market studies are given, while deeper economic assessments fed section 4 of this report.

3.6.1 Autorité de la concurrence (FR) market study

In June 2023, the Autorité de la concurrence issued its opinion on completion of its market study on competition in the cloud computing sector.[106] This study focuses particularly on cloud layers relating to IT infrastructure (IaaS) and platform services (PaaS) for business customers, but also looks at the entire cloud value chain including software where relevant to the competitive analysis. Further, the French Competition Authority analysed three types of related areas in which market power could potentially be leveraged: data centre colocation services, on-premise software, and intermediation in consulting and integration of cloud solutions.

The dynamics for cloud computing services in France are similar to other EU countries, characterised by three large cloud service providers (AWS, Microsoft Azure and Google Cloud), which, according to the Authority, could impede a new operator from growing rapidly. There are also other competitors such as data centre operators, 'pure player' cloud providers, providers aiming to offer certified 'trusted cloud' services, and IT service companies that act as integrators. The French NCA identifies specific competitive risks related to:

- Migration of on-premise information systems to the cloud, such as restrictive contractual clauses tied sales, pricing advantages and technical restrictions favouring current software provider products (for which the French NCA considers necessary to devote particular vigilance to software markets and their relationships with cloud services markets);
- migration from one cloud service provider to another, such as the lack of data portability and commercial conditions that 'lock-in' customers, including through software licensing; and

[106] Autorité de la Concurrence, 2023 (n 5).

- barriers to expansion for large suppliers' competitors, such as suppliers' presence in related markets and the provision of more advantageous commercial or technical conditions for their own products, restricted access to marketplace, and a lack of interoperability.

During the French NCA's public consultation, a number of players also identified risks deriving from concentration in the cloud sector, which could reinforce a general negative impact on competition through reducing the number of players, potentially bundled or tied sales strategies, a lack of innovation, and potentially higher prices or declining quality. However, the entry into force of the DMA should enable competition authorities, and in particular the European Commission, to monitor more closely those acquisitions that currently escape merger control.

In general, the French NCA is of the opinion that adoption of the DMA, the Data Act, and the draft national law to secure and regulate the digital space might be better suited to address those problematic situations and reduce competitive risks. In particular, the Autorité believes that such instruments are better suited to address any market failures. However, with respect to the Data Act, it notes that it would be appropriate to monitor several issues as the European Commission is due to carry out an evaluation of legislation in three years, including:

- distinguishing the regime applicable to egress fees from other migration costs,
- carrying out an impact study on cloud credits, and
- specifying measures to promote portability and interoperability.

As for the national French draft legislation, the Authorité issued an opinion,[107] making a number of recommendations designed to ensure that the French draft legislation's provisions are aligned with those of the Data Act to strengthen its effectiveness. In any event, the French NCA underlines that, besides regulatory obligations, competition law (as well as the legislation about abuse of economic dependence and the Code of commerce provisions about unfair practices) is a particularly useful tool to preserve and stimulate competition in the digital economy, because of its flexibility and comprehensiveness which allow both to define, detect, and sanction new practices and to adapt well-established pro-competitive remedies to 'new' digital services. Furthermore, there are amendments filed to the draft French law to address the issue of software licensing reported by the French competition authority.

3.6.2 ACM (NL) market study

In September 2022 the ACM issued a final document resulting from a market study investigating whether competition for cloud services is functioning properly, and whether there are any risks to prices, quality, and innovation, possibly caused by market structures or by commercial practices and technical settings. [108]

ACM analyses the cloud services sector, where services are offered by some of the largest companies in the world, such as Amazon, Microsoft, and Google, which are active on the IaaS, PaaS, and SaaS layers, so they are vertically integrated. The two largest competitors both in the Netherlands and in Europe, Microsoft Azure and Amazon Web Services (AWS), have very large market shares on the IaaS

[107] Autorité de la Concurrence (2023b) Opinion 23-A-05 on the draft law to secure and regulate the digital space
[108] ACM, 2022 (n 5).

and PaaS layers (35 to 40 percent). Google is the third competitor in the market, but a very strong one. Other active market participants in the European and Dutch cloud services market include IBM, Oracle, VMware, OVHcloud, Scaleway, and the Dutch company Leaseweb.

The market study focuses on business users, that is, companies and organisations (public and private) that purchase cloud services. Another important group of users that is considered, is composed of independent software vendors (ISVs): companies that develop IT services and offer them to end users as SaaS services, for example, via the marketplace of cloud providers and built on their IaaS and/or PaaS environment.

ACM underlines the importance of the initial moment of choice by a customer, when there is stronger competition, for example with large amounts of credits. ACM then describes the advantages (services that can work together optimally and volume discounts) and disadvantages (path dependence) of choosing one specific cloud provider with an integrated offer. However, it describes that many companies purchase services from different cloud providers (multi-cloud).

After the first moment of choice, ACM highlights that vendor lock-in may emerge, because of different kind of switching barriers, be it technical (closed APIs or different standards), organisational/procedural (lack of interoperability), or financial/monetary (egress fees).

ACM clearly distinguishes between data portability (that concerns the transfer of data) and interoperability (that involves repeated communication between services of different providers). It highlights that poor interoperability reinforces vendor lock-in. The market study also notes that it expects increasing consolidation of cloud services to continue as a result, among other reasons, of economies of scale and network effects.

Increasing consolidation coupled with switching barriers and poor interoperability increase users' dependence on just a few vertically integrated cloud providers. This applies to both the end-users and companies that offer cloud services on the infrastructure of the major players (ISVs). ACM is of the opinion that the Digital Markets Act, the proposed Data Act, and the Dutch Competition Act are relevant legal instruments to address the risks outlined and promote open markets. In addition, ACM proposes the following amendments to the Data Act (referring to the initial Commission proposal):

- to make a clear distinction between data portability and interoperability;
- to mandate APIs to be publicly available, in order to facilitate interoperability;
- to mandate that different service types can communicate with each other, enlarging the scope of application of the proposed requirements for standards;
- to lower egress fees, not only in the case of portability but also in the case of interoperability, allowing to charge only for the specific costs incurred for interoperability; and
- to allow third-party service providers to interconnect their services with services of another cloud provider with the same quality as services within a specific cloud.

3.6.3 Ofcom (UK) market study

In October 2022 Ofcom initiated a market study, under the 2002 UK Enterprise Act as amended by the 2013 Enterprise and Regulatory Reform Act, and submitted its interim report to public consultation in

May 2023.[109] The interim market study report found high concentration of cloud infrastructure services as well as potential barriers to competition driven by practices that make it difficult for business customers to switch cloud provider or use multiple providers. For this reason, the interim report proposes a referral to the UK Competition and Markets Authority (CMA) for a market investigation.[110]

The final report, considering all the responses received by Ofcom within the public consultation, was published on the 5th of October.[111] This final report found that, while there are some positive signs of competition, there are also clear indications that the cloud infrastructure market is not working well because of market features that have an adverse effect on competition. On this basis Ofcom exercised its discretion and referred the market for public cloud infrastructure services to the CMA to carry out a market investigation. CMA has powers to impose legally binding remedies/obligations upon conclusion of a market investigation, in case the market investigation highlights that the cloud services sector is not properly functioning.

Ofcom's report focuses on 'cloud infrastructure services' (comprising IaaS and PaaS). The interim report found that in the UK there are two leading providers of cloud infrastructure services: Amazon Web Services (AWS) and Microsoft, who had a combined market share of 70% to 80% in 2022. Google is their closest competitor with a share of 5% to 10%. A diverse set of independent software vendors (ISVs) build their products on cloud infrastructure from those main infrastructure operators, yet also compete directly with some of their services.

As mentioned, Ofcom's report found evidence of competition in cloud infrastructure, especially when providers are competing to attract new customers (moving to the cloud for the first time), which contributes to benefits for customers, including product innovation, discounts, and a wide choice of software services from ISVs. Nevertheless, Ofcom found that competition for customers to switch and use multiple suppliers ('multi-cloud') is limited by some commercial/technological features and practices. The most concerning are:

- egress fees, which make switching more costly and thus soften competition dynamics and discourage customers from using more than one cloud provider;
- technical restrictions on interoperability and data portability, which imply that customers need to put additional effort into reconfiguring their data and applications to work on different clouds; and
- committed spend discounts, which can reduce customers' costs, yet possibly, depending on discounts structures, disincentivise customers to use multiple cloud providers.

Therefore, Ofcom's Report highlights that there are indications these market features are already causing consumer harm. In this scenario, Ofcom is concerned by lock-in by market leaders further dampening competition for new and existing customers. This could have implications for ISVs, especially where they become more dependent on the market leaders for access to customers.

[109] Ofcom, 2023 (n 6).
[110] Ofcom (2023c) Public cloud infrastructure services: Proposal to make a market investigation reference
[111] Ofcom (2023d) Statement: Cloud services market study (final report)

In addition, Ofcom has received and preliminarily evaluated concerns regarding the software licensing practices put in place by an integrated cloud provider. In particular, those concerns were about how software products used by businesses are sold and licensed by that integrated company, providing both software and cloud services, in order to make it less attractive for customers to use those licensed software products on the cloud infrastructure of competitors. Ofcom is of the opinion that it is possible that the alleged conducts could risk dampening competition in cloud infrastructure services. However, Ofcom has not made any definite findings, leaving to the CMA's to decide whether this issue should be deeply investigated in order to ascertain any possible anticompetitive impact of the software licensing practices on competition in cloud infrastructure.

4. ECONOMIC ANALYSIS OF COMPETITION ISSUES IN CLOUD COMPUTING

The review of European policy initiatives demonstrates that several of the recent interventions have been motivated by concerns about the well-functioning of markets in cloud computing. In this section, we analyse specific characteristics and issues of the cloud computing industry from an economic perspective and evaluate whether these can have a negative impact on effective competition in cloud computing. In our analysis, we focus on whether *vendor lock-in* and *economies of scale and scope* give rise to market failures, that is, market outcomes that deviate from the first-best outcome that would maximise social welfare. In this context, it is important to note that from an economic perspective, the identification of a market failure presents a necessary condition for regulatory intervention, as it indicates that market outcomes can in principle be improved. However, a market failure should not serve as an unconditional justification for regulatory intervention on its own. First, regulation may not be able to restore the first-best market outcome but can only imperfectly address the competition issue. Second, regulation and its implementation are associated with welfare costs, which are important to consider when evaluating the net benefit of intervention. Third, regulation may yield unintended side effects and face complex implementation challenges due to imperfect information and uncertainty in practice. In consequence, regulatory intervention involves economic trade-offs that should be considered with respect to their impact on market outcomes and the different stakeholders. We turn to the analysis of these trade-offs for specific regulatory approaches and interventions in the context of cloud computing in Section 5.

4.1 Vendor Lock-in

Customers' decision to migrate their computing resources into the cloud involves a central trade-off between the expected business benefits for the customer and the loss of ownership and direct control over its computing resources. This is a typical 'make-or-buy' decision, which is addressed by considering different types of transaction costs. As customers cede ownership of their computing resources to the external cloud provider, there exists the risk of *vendor lock-in*. In general, vendor lock-in arises "when the extra value […] from a new supplier's products or services is exceeded by the cost of switching from [the] current vendor".[112] In consequence, the customers' future business opportunities can be limited by their dependency on the cloud provider.[113]

Vendor lock-in can lead to market failure if switching costs allow suppliers to raise prices above the competitive level without having to fear the churn of their customers. Thus, lock-in can undermine the competitive process in a market over the long run when switching costs make it unprofitable for providers to poach customers from their competitors. Hence, it is an explicit goal of the Data Act to mitigate potential vendor lock-in (see Section 3.2). However, high switching costs and the prospect of vendor lock-in can at the same time intensify competition to attract customers in the first place. This

[112] Lookabaugh, T., & Sicker, D. C. (2004). Security and Lock-in. In *Economics of Information Security* (pp. 225-246). Boston, MA: Springer US.
[113] Arce, D. (2022). Security-Induced Lock-In in the Cloud. *Business & Information Systems Engineering*, *64*(4), 501-513 ; Satzger, B., Hummer, W., Inzinger, C., Leitner, P., & Dustdar, S. (2013). Winds of change: From vendor lock-in to the meta cloud. *IEEE internet computing*, *17*(1), 69-73.

is because "early sales induce lucrative follow-on sales" and suppliers compete ex-ante for ex-post market power over a customer.[114] In consequence, markets with high switching costs and vendor lock-in are often characterised by "bargain-then-ripoff" pricing, as termed by the economic literature.[115] In this vein, suppliers may not only compete for the initial sale to a customer but for a series of follow-up sales by the same customer. Thus, conventional competition in the market can be replaced by a mode of competition for the market with respect to each individual customer.[116] Hence, in the presence of switching costs and vendor lock-in, harm from higher prices in the long term has to be weighed against benefits from lower prices in the short term. In general, nonetheless, switching costs lead to less competitive markets.[117] For example, ex-ante benefits may not fully compensate for later price increases in markets where (i) there is one (or few) technological first mover(s), (ii) market power can be leveraged by a dominant firm from adjacent markets, or (iii) oligopolistic competition could result in collusive practices.

Vendor lock-in may not only affect allocative efficiency through the effects on vendors' pricing but can also entail effects on dynamic efficiency and innovation. In particular, vendor lock-in may obstruct the efficient matching of vendors and customers when customers decide not to switch because of high switching costs.[118] In consequence, this can lower innovation adoption by customers as well as innovation incentives of suppliers and therefore have negative effects on productive efficiency.[119] In particular, locked-in customers have only limited access to innovation, when such innovation is available at a competing vendor but not at their current vendor or innovation is available for a complementary, yet incompatible, product. In turn, vendors' incentive to engage in innovation activities decreases if the base of potential adopters is diminished by vendor lock-in.[120] Overall, this can lead to negative effects on the variety of available services and products as a consequence of vendor lock-in.[121]

In general, switching costs are present in many markets and for many goods. Their significance depends on market characteristics and business practices, which therefore ultimately determine whether switching costs can amount to vendor lock-in. In the following, we discuss the characteristics and practices that are of particular relevance for switching costs in the context of cloud computing services.

4.1.1 Relation-specific investments and learning effects

The configuration, deployment, and operations of IT infrastructure and software applications require relation-specific investments from customers. This is especially the case for more complex infrastructure and software architectures of business customers, as those must frequently be configured and adjusted to the precise needs and policies of a customer's organisation, which can be very diverse across customers. For instance, customers must frequently customise and configure

[114] Farrell, J., & Klemperer, P. (2007). Coordination and lock-in: Competition with switching costs and network effects. In M. Armstrong & R. Porter (Eds.), *Handbook of Industrial Organization - Volume 3* (pp. 1967-2072). North-Holland.
[115] Ibid, p. 1972.
[116] Ibid.
[117] Ibid; Klemperer, P. (1987). Markets with consumer switching costs. *The Quarterly Journal of Economics*, *102*(2), 375-394.
[118] Farrell & Klemperer, 2007 (n 115).
[119] Lookabaugh & Sicker, 2004 (n 113).
[120] Ibid.
[121] Farrell & Klemperer, 2007 (n 115).

operating systems and applications to implement security features and authentication mechanisms required by their organisation's security policies and user management. Furthermore, there usually exist numerous technical dependencies between the different hardware and software components of a customer's system that must be managed and accounted for when individual components are changed or exchanged. Once a customer undertakes these activities and investments (which may include money, time, and effort from the customer), they are usually sunk and cannot be re-purposed to support any other transaction.

Although relation-specific investments can also accrue for IT infrastructure or applications supplied through self-provisioning, traditional outsourcing, or one-time purchases, they are particularly relevant for cloud computing services.[122] This is because a customer's effort in configuring and adapting its cloud services is usually not directly transferable when switching to other cloud providers due to provider-specific requirements, technical incompatibilities between service providers, or customers' inability to easily access and port such configurations and other customer-generated metadata. In the case of more complex service ensembles, relation-specific investments do not only arise for individual services but also for the configuration and management of the interplay between services. Customers may also invest in additional 'meta services' to monitor the consumption and costs of their cloud services that can be purchased directly from the cloud provider, procured from third parties, or built as customers' own solutions.[123] Furthermore, customers may optimise their IT architecture and associated business processes based on the services offered by a specific cloud computing provider. For example, when Netflix decided to migrate its IT infrastructure to the AWS cloud it took eight years to implement a "cloud-native approach, rebuilding virtually all of [their] technology and fundamentally changing the way [they] operate the company".[124]

In addition, the adoption and use of a cloud services give rise to learning effects as customers become more familiar with the services of a specific provider and develop technical expertise in setting up, configuring, and monitoring these services.[125] Learning effects can thus represent a particular type of relation-specific investment, as they increase the costs of a customer when switching to a different service provider with new interfaces, other proprietary services, or different technical implementations. The different certification programs for cloud engineers offered by hyperscalers are an indication of the relevance of cloud provider-specific knowledge and the importance of this expertise for business customers.[126] Moreover, in the UK, customers rated the need to retrain staff as the second most important challenge of switching to a different IaaS or PaaS service provider (33% of all respondents) according to Ofcom.[127]

[122] Makhlouf, R. (2020). Cloudy transaction costs: a dive into cloud computing economics. *Journal of Cloud Computing*, *9*(1), 1-11; Nuseibeh, H. (2011). Adoption of cloud computing in organizations. *Proceedings of the Seventeenth Americas Conference on Information Systems*. Detroit, Michigan, USA.
[123] Mahklouf, 2022 (n 47).
[124] Netflix, 2016 (n 24).
[125] Ofcom, 2023 (n 6).
[126] AWS Certification https://aws.amazon.com/certification/; Microsoft Learn for Azure https://learn.microsoft.com/en-us/training/azure/
[127] Ofcom (2023b). Cloud services market study. Interim report, annexes 5 to 8, p. 48. https://www.ofcom.org.uk/__data/assets/pdf_file/0028/256456/cloud-services-market-study-interim-report-annexes-5-8.pdf

4.1.2 Data-induced switching costs

A peculiar type of switching costs of digital services in general and cloud computing in particular are data-induced switching costs.[128] Data-induced switching costs arise when relevant data is generated while using a service but the data is not readily portable to another provider (see the related provisions in the Data Act as discussed in Section 3.2.5). For cloud computing services these switching costs can arise from a customer's loss of physical control over its data, if the data is difficult and costly or even impossible to export from the cloud service.[129] At the IaaS layer, customers can usually access the data that was imported by the customer and data created during the use of the service.[130] Customer-generated metadata such as the configuration parameters of virtual machines may be more difficult to access for the customer, as such data is often under the exclusive and proprietary control of the cloud provider. As a result, customers then have to re-enter such metadata manually when switching cloud providers, which can result in transaction costs for configuring the new services at the destination service provider to replicate the services at the original service provider. These costs of imperfect data portability contribute to the overall switching costs for customers and may thus discourage switching. For example, 30% of UK customers indicated "technical difficulties in transferring data" as a challenge of switching between IaaS or PaaS services according to market research by Ofcom.[131] In this context, it has been noted that the export of metadata would not be useful for customers, as this data often relates to proprietary services and thus, cannot be directly imported and processed by the destination service provider. However, even in the case of data incompatibility, the data could be made exportable in a structured, machine-readable data format by the original service provider such that the customer or potential destination service providers could automate the extraction of relevant information for the new service or develop technical wrappers that allow for automated conversion of the data into a compatible data format. Hence, the exportability of customer-generated metadata in a proper data format may at least have some value in reducing switching costs for customers.

The relevance of data-induced switching costs is magnified at the SaaS layer when services do not allow customers to fully export the data that they have imported or that was created during the use of the service. Support for data export functions and data portability differs between SaaS service providers and even within specific SaaS services.[132] Whereas customer data at the IaaS layer is often homogeneous and stored in a uniform and structured manner (for instance, all data stored in a database service), customer data at the SaaS layer is often more heterogeneous and diverse (for example, messages, documents, notes, contacts, calendar entries of users in an office suite). Furthermore, functionalities between SaaS services are often differentiated, both in terms of their precise feature set as well as their technical implementation. Hence, even if data can be exported at

[128] Wohlfarth, M. (2019). Data portability on the internet: an economic analysis. *Business & Information Systems Engineering*, *61*, 551-574 ; Krämer, J., & Stüdlein, N. (2019). Data portability, data disclosure and data-induced switching costs: Some unintended consequences of the General Data Protection Regulation. *Economics Letters*, *181*, 99-103 ; Lam, W. M. W., & Liu, X. (2020). Does data portability facilitate entry?. *International Journal of Industrial Organization*, *69*, 102564.

[129] Marston et al., 2011 (n 47).

[130] See, e.g., Ofcom, 2023, p. 82 (n 6).

[131] Ibid.

[132] See, e.g., Slack, which makes different scopes of data available depending on the customers' subscription plan, https://slack.com/help/articles/204897248-Guide-to-Slack-import-and-export-tools

the original service it can often not be directly imported at a destination service.[133] Incompatibility and barriers to exportability may be further promoted by a cloud service provider's incentive to raise switching costs by collecting and storing data in ways such that they are not easily transferable to a competing cloud service provider.[134] Customer difficulties in porting data due to incompatible data formats and heterogenous service functionalities can to some extent be alleviated by support and technical assistance from destination cloud service providers that have an incentive to facilitate the transfer and import of customer data.[135] In addition, there exist third-party services that may support data portability for popular SaaS services.[136] However, even if technical solutions exist, transaction costs in terms of additional effort, financial costs, and risks associated with data portability challenges can represent significant data-induced data switching costs, which lower customers' propensity to switch. For instance, at the IaaS and PaaS layers, "time and cost of making the change", which is directly influenced by data-induced switching costs, was rated the most important challenge of switching cloud service providers by UK customers.[137]

4.1.2 Technical incompatibility

Incompatibility of substitute services across cloud providers

Technical incompatibility between services of different cloud providers can increase the switching costs of customers in two main ways. First, technical incompatibility of functions and interfaces can make it more difficult for customers to replace a specific individual service at the original cloud service provider with the service of a destination cloud provider (see also Sections 3.2.2 and 3.2.7 on related provisions in the Data Act that aim to address technical barriers to switching through interoperability regulation). Incompatibility between services from different cloud providers can arise from the high diversity of cloud services and their differentiated feature set as well as their different technical implementations. Furthermore, incompatibility may be reinforced by the deliberate and strategic design decisions of a cloud service provider. Thus, "application portability"[138] between cloud providers is often not feasible without additional modifications of the service and effort of the customer, which can create considerable switching costs for a customer. According to Ofcom, 58% of IaaS/PaaS customers in the UK using public cloud indicated at least one technical challenge among data portability, application portability, and interoperability as a barrier to switching.[139]

In this context, it is important to note that there exist considerable differences between technical implementations of cloud services. On the one hand, there are several popular open-source implementations for services especially at the PaaS layer that are supported by the majority of cloud service providers.[140] Switching is easier from a technical perspective in this case, as services at the

[133] See, e.g., on data migration from Slack to Microsoft Teams: Integrated Research (n.d.) How To Successfully Perform A Slack To Teams Migration https://www.ir.com/guides/slack-to-teams-migration-guide; Kent (n.d.) Need to Migrate from Slack to Microsoft Teams? You don't have to! https://dispatch.m.io/migrate-slack-to-microsoft-teams/

[134] Cf. Wohlfarth, 2019 (n 129).

[135] See, e.g., Microsoft (2023). Migrate from Slack to Microsoft Teams https://learn.microsoft.com/en-us/microsoftteams/migrate-slack-to-teams

[136] See, e.g., Kent (2021). 4 Options For Migrating Slack To Microsoft Teams https://techcommunity.microsoft.com/t5/microsoft-teams-community-blog/4-options-for-migrating-slack-to-microsoft-teams/ba-p/2677044

[137] Ofcom, 2023b, p. 48 (n 128).

[138] Kolb & Wirtz, 2014 (n 21).

[139] Ofcom, 2023, p. 95f (n 6).

[140] See, e.g., MongoDB https://www.mongodb.com/atlas/database

different providers share key features, service characteristics, and technical implementations. Nonetheless, services may still need to be adapted and reconfigured to the environment of the destination cloud provider and thus require relation-specific investments. On the other hand, there exists a range of proprietary solutions, sometimes for the same type of services as the open-source solutions, with different cloud providers (and especially hypersalers) offering their own service. These proprietary services may offer additional features or better integration with the cloud provider's complementary services. For example, AWS advertises that its service Amazon DocumentDB, an alternative to the open-source solution MongoDB, "simplifies [a customer's] architecture by providing built-in security best practices, continuous backups, and native integrations with other AWS services".[141] However, these proprietary services will regularly be more difficult to replicate at a destination service provider, as they offer specific feature sets, do not rely on open-source reference architectures, and are more tightly integrated with the specific environment of the original cloud service provider.

Therefore, switching costs of customers from technical incompatibility can also be influenced by the adoption and technical migration decisions of a customer. In particular, when open-source solutions are available as alternatives to proprietary solutions for specific service types, a customer can strategically aim to reduce its technical dependency on the cloud service provider. This may come at the cost of a lower technical performance, higher costs, or less efficient integration with other services. Nonetheless, as long as these disparities are not too stark, a customer can implement open policy strategies to minimise reconfiguration efforts for switching cloud service providers. Whether such open policy strategies can constitute effective instruments against technical vendor lock-in then depends on the availability of open-source services at cloud service providers, the commercial terms for their usage (especially regarding price differences to proprietary services), and other technical obstacles to migrating an application (see, for instance, data-induced switching costs as discussed in the previous section). Naturally, these conditions are, to a large extent, under the control of the cloud service provider, which can give rise to concerns that service providers with a large customer base have the incentive to steer customers towards proprietary, less interoperable solutions.[142] At the same time, it is important to consider that incompatibility can be the outcome of competition and innovation activities, as cloud providers aim to differentiate themselves from competitors.

In general, porting a single, stand-alone cloud service is significantly easier for a customer than porting an ensemble of services that may involve complex dependencies between services.[143] In the case that a single service of an ensemble is migrated to a different cloud provider, technical switching costs will additionally depend on the interoperability between the different services, which we discuss next.

Incompatibility of complementary services across cloud providers

Besides the portability of a service, technical incompatibility can make it more difficult for customers to interconnect services of different cloud providers. A lack of interoperability therefore hampers a customer's ability to operate a multi-cloud that combines and interconnects services from different cloud service providers. In general, customers may want to adopt multi-cloud architectures because

[141] AWS (2023). Amazon DocumentDB–How it works https://aws.amazon.com/documentdb/?nc1=h_ls
[142] Ofcom, 2023, p. 103 (n 6).
[143] See also Ofcom, 2023, p. 99 (n 6).

of a range of different motivations and reasons (for example, among others, to ensure service reliability, take advantage of specific service features, or reduce dependency on a specific provider). Interoperability for multi-cloud support is particularly important if the customer wants to migrate a specific service to another service cloud provider but retain other services of the service ensemble at the original service provider. In this use case, inter-vendor interoperability directly affects the switching costs for migrating a service. While interoperability can facilitate interconnection, the feasibility of multi-cloud solutions will also be impacted by the operational challenges inherent to transferring data between locations and providers (such as latency, data consistency and security challenges).

In case interoperability across cloud providers is technically unfeasible or economically unviable from the perspective of a customer, additional switching costs can arise from a customer's need to provision a group or series of compatible services. This "creates economies of scope among [the] purchases from a single [cloud provider]"[144] resulting in an increased incentive for customers to purchase all of its cloud services from the same provider. In consequence, the decision to switch to an alternative cloud provider is no longer confined to a single service but is based on the entire ensemble of interconnected services run by a customer. A lack of interoperability has therefore been argued to represent a competitive disadvantage for smaller cloud service providers and market entrants when they offer only specialised services and customers must procure complementary cloud services from other providers.[145] At the same time, there is a natural economic incentive for providers with a larger customer base to seek incompatibility with other providers to sustain their competitive advantage, whereas providers with a smaller customer base have the incentive to be interoperable with larger providers in order to be able to attract and poach their customers.[146]

Market research indicates that interoperability represents a concern for a significant share of customers. For example, in the UK, "52% of customers cited a lack of interoperability between different IaaS/PaaS providers' services as a key concern with the cloud infrastructure services market".[147] In particular, "moving data across providers" has been cited by these survey respondents as the most important challenge of using multi-cloud (45% of all respondents), although this may also include non-technical obstacles to interconnection.[148]

ISVs and competing cloud providers have raised concerns that hyperscalers may limit the interoperability of their cloud service offerings, for instance, through the design of non-open APIs and modifications of open-source solutions.[149] Moreover, hyperscalers offer a range of proprietary services that feature limited interoperability. However, there are also technical justifications for the design of incompatible services. First, as discussed above, the technological heterogeneity of cloud computing services can be the result of the diverse demands and needs of customers. Generic and

[144] Farrell & Klemperer, 2007, p. 1971 (n 115).
[145] Autorité de la concurrence, 2023 (n 5).
[146] Calvano, E., & Polo, M. (2021). Market power, competition and innovation in digital markets: A survey. *Information Economics and Policy*, *54*, 100853; Crémer, J., Rey, P., & Tirole, J. (2000). Connectivity in the commercial Internet. *The Journal of Industrial Economics*, *48*(4), 433-472.
[147] Ofcom, 2023, p. 85 (n 6).
[148] Ofcom, 2023b, p. 41 (n 128).
[149] Ofcom, 2023, p. 103 (n 6); Ranjan, R. (2014). The cloud interoperability challenge. *IEEE Cloud Computing*, *1*(2), 20-24.

homogeneously standardised solutions do often not satisfy the requirements of large firms, due to their unique, large, and complex business processes and information systems, as well as of smaller firms, due to their specialisation and focus on niche markets.[150] Second, technical innovations may not only occur at the individual service level but also at the system level, that is, cutting across services. For example, AWS offers its service AWS Lambda to offer support for serverless computing and function as a service (FaaS) across AWS cloud services.[151] This can facilitate implementation for customers of AWS, but is technically difficult to integrate into services outside the AWS ecosystem. The same holds for other cross-cutting services that require precise knowledge of the executing environment and the technical implementation of the respective services.

In general, there exists a variety of technological solutions to circumvent technical obstacles to interconnection offered by both third parties and cloud service providers. For instance, hyperscalers offer tools and services that can support customers in establishing multi-cloud solutions (see the Unified operations approach[152] and the service Azure Arc[153] offered by Microsoft, for instance). In this case, the respective cloud service provider usually remains the main gateway to the services of other providers. Third parties, such as Snowflake, offer technical solutions that aim to implement additional abstraction layers to span across different cloud service providers. For example, Snowflake[154] provides a data warehouse service that is interoperable with IaaS and PaaS services of the different hyperscalers and thus promotes itself as the "Data Cloud".[155] To achieve such interoperability, it is usually necessary, from a technical perspective, to add an additional technical layer that abstracts from the underlying vendor-specific functionalities and/or to implement vendor-specific adaptors to allow for the exchange of messages between otherwise incompatible interfaces. The benefits of interoperability thus come regularly at the cost of additional technical overhead and architectural complexity.

Thus, similar to the considerations on maintaining compatibility for switching, customers are faced with strategic adoption decisions regarding multi-cloud architectures. In particular, there exist technical approaches to maintain more interoperability and flexibility. However, these interoperability advantages often come at the cost of more technical complexity, lower efficiency, and higher costs. Customers need to take these issues into account for an effective implementation and must weigh them against the short-term and long-term benefits of multi-cloud solutions (such as being less dependent on a single provider or being more resilient in the case of service outages). In addition, maintaining interoperability is particularly challenging for a customer if the provisioned cloud services are subject to frequent changes that may also alter the specifications of interfaces or the message

[150] Tripathy, S., Sengupta, A., & Jyotishi, A. (2023). Looming market failure in cloud computing: a new institutional economics perspective. *Digital Policy, Regulation and Governance 25*(5) 409-504.
[151] AWS (2023). AWS Lambda– Run code without thinking about servers or clusters. https://aws.amazon.com/lambda/
[152] Microsoft (2022). Unified operations for hybrid, multicloud, and edge. https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/scenarios/hybrid/unified-operations
[153] Microsoft (2023). Azure Arc https://azure.microsoft.com/de-de/products/azure-arc; Microsoft (2023). Azure Arc overview https://learn.microsoft.com/en-us/azure/azure-arc/overview
[154] Snowflake (2023). Snowflake Data Cloud. https://www.snowflake.com/en/
[155] Snowflake (2023). The Snowflake Platform. https://www.snowflake.com/en/data-cloud/platform/

format that is expected as an input or given as an output by a specific service.[156] Hence, interoperability usually incurs continuous costs, whereas portability is associated with a fixed cost at the time of switching.[157] In consequence, customers may adopt proprietary and integrated solutions due to their performance or cost advantage, despite the risk of lesser interoperability. The temptation for customers is illustrated by the following quote by Leong, an Industry analyst, who stated in the context of multi-cloud failover that "the huge cost and complexity of a multicloud implementation is effectively a negative distraction from what [customers] should *actually* be doing".[158]

4.1.3 Financial switching costs

Customers of cloud computing services incur direct financial switching costs if they have to pay for the transmission of data from the original service provider to the destination service provider (and possibly for having to pay for both cloud services concurrently while in the process of switching.). In the cloud computing industry, some providers including the hyperscalers charge for the transfer of data. This can concern data flows between services within the ecosystem of a cloud provider, data flows to the customer, and data flows across cloud providers.[159] There are commonly no ingress data fees, that is, customers do not pay for incoming traffic to their cloud services or for uploading data. From a competition perspective, data egress fees that apply to outgoing data traffic of the current cloud provider's ecosystem are of particular concern.[160] First, these egress fees increase the costs of a switching provider and make switching between cloud providers less attractive if switching requires the transfer of significant volumes of data (see also Section 3.2.4 on related provisions in the Data Act). The volume of customer data and thus the amount of switching costs due to egress fees will vary significantly between different types of customers and different types of services.[161] Second, as egress fees are usually higher than fees for internal data flows within a provider's ecosystem, egress fees increase the costs of multi-cloud architectures for customers. This is because every data flow that is exchanged between services across providers is more costly than data flows within a provider's service ecosystem. Whereas in the case of switching, egress fees amount to a one-time fixed cost, they represent variable costs in the case of interoperability and can thus, for example, increase with the demand for the customer's service. A higher cost for multi-cloud solutions may incentivise customers to provision services from a single provider, which in turn can increase switching costs due to the need to replace the entire ensemble of services in case of switching providers.[162]

Differentiated pricing of internal and external data flows may be justifiable on the grounds of different costs that the cloud service provider incurs for these data transfers. In particular, internal data transfers will regularly incur (close to) zero marginal costs, as the underlying network infrastructure is owned by the cloud service provider and is financed by fixed-cost investments. In contrast, marginal costs for external data transfers are usually positive as they often require transmission over third-

[156] See Section 2.1.1 and Schnurr, 2023, (n 17) for a brief summary of the technical characteristics of cloud computing services, of which many are subject to frequent updates and changes.
[157] Cf. Ofcom, 2023 (n 6).
[158] L. Leong (2021). Multicloud failover is almost always a terrible idea. https://blogs.gartner.com/lydia_leong/2021/10/14/multicloud-failover-is-almost-always-a-terrible-idea/
[159] Ofcom, 2023, p. 109 (n 6).
[160] ACM, 2022 (n 5); Ofcom, 2023, p. 85 (n 6).
[161] Ofcom, 2023, p. 113 (n 6).
[162] See the discussion on incompatibility of complementary services in the previous section and also Farrell & Klemperer, 2007 (n 115).

party networks that demand a transit fee that is proportional to the volume of the transferred data. However, in current practice, the egress fees of hyperscalers have been found to be several times higher than those of competitors.[163] Moreover, data egress fees of hyperscalers have generally stayed relatively flat over recent years.[164] This raises concerns that higher egress fees do not only reflect cost differences but that they are used as a strategic instrument to increase the costs for customers for switching and interconnecting services across providers.[165] That pricing of data flows involves strategic considerations beyond a pure cost basis is also indicated by zero ingress fees.[166] In general, such a pricing scheme is in line with a provider's economic incentives to attract new customers and data in-flow, and retain them within its own service. In fact, incentives to differentiate ingress and egress fees may be reinforced by competition, as indicated by AWS's decision to stop charging ingress fees after Microsoft entered the cloud market.[167] From a theoretical view, it is also intuitive that providers with a larger user base have an incentive to set higher egress fees than providers with a smaller user base, as they have a higher opportunity cost for lowering switching costs, similar to the considerations with respect to (in)compatibility.[168]

For an overall evaluation, of the impact of egress fees on vendor lock-in, it is important to consider the customers as strategic agents as well. Although it has been argued that customers may have difficulties in predicting their data growth and the associated costs, it is reasonable to assume that business customers with larger traffic flows that are most affected by egress fees will have a good understanding of the expected costs related to external data flows.[169] In particular, egress fees are usually transparently documented on a cloud provider's website. Hence, customers can be expected to include these costs in their cost-benefit analysis when making an adoption decision. In this context, very large customers (who would likely also suffer most from data egress fees) may be able to negotiate more favourable terms and prices when making their initial adoption decision.[170] In addition, customers may benefit from discounts offered by destination service providers in the case of switching that can offset part of the financial switching costs from egress fees. In general, strategic adoption by customers will put at least some limit on the egress fees that can be charged by cloud providers, although competition may at the same time promote a differentiation of ingress and egress fees. Thus, egress fees may have the most meaningful impact on customers' switching costs by making it more costly to establish multi-cloud architectures and favouring the provision of service bundles from a single cloud provider than by directly increasing the costs of switching through increased costs for data and application portability. As discussed above higher costs of multi-cloud approaches for customers may to some extent be explained by the higher underlying costs of external data transfers for cloud service providers, but additional cost asymmetries could further discourage multi-cloud approaches.

[163] ACM, 2022 (n 5); Ofcom, 2023 (n 6).
[164] ACM, 2022, p. 59 (n 5); Ofcom, 2023, p. 120 (n 6).
[165] Autorité de la concurrence, 2023 (n 5).
[166] Actual costs for data traffic inflow are, e.g., instead settled with storage costs (ACM, 2022, p. 59)
[167] Ofcom, 2023, p. 122 (n 6).
[168] Laffont, J. J., Rey, P., & Tirole, J. (1997). Competition between telecommunications operators. *European Economic Review*, *41*(3-5), 701-711. Laffont, J. J., Rey, P., & Tirole, J. (1998). Network competition: II. Price discrimination. *The RAND Journal of Economics*, 38-56.
[169] See Ofcom, 2023, p. 133f. (n 6) for different perceptions of customers on the challenge to predict cloud spend.
[170] See Ofcom, 2023, p. 122 (n 6).

4.1.4 Cloud credits and committed spend discounts

Cloud credits

Many cloud providers, including the hyperscalers, offer cloud credits that "provide customers with a spending allowance on eligible services".[171] Commonly, there are two types of credits:[172]

- *Short-term credits* (usually up to three months) are used by cloud providers to entice new customers or promote the takeup of new services.[173] Alternatively or additionally, cloud providers may offer free trials or free tiers for a limited period of time.[174]
- *Long-term credits* (possibly for several years with a maximum range of USD 100,000 to USD 200,000 offered by the hyperscalers according to Ofcom[175]) for selected customers, especially start-ups, can motivate growing firms to adopt a cloud service provider early and grow as a cloud-native business.

Cloud credits represent an immediate benefit for eligible customers as they directly reduce the costs for initial cloud migration or for switching providers. Thus, cloud credits can be viewed as a pricing instrument that allows providers to compete more fiercely for new customers without incurring opportunity costs for lowering prices for the entire customer base. Such pricing schemes are common in many markets and particularly typical for markets where customers have switching costs.[176] Offering new customers free allowances and discounts has several pro-competitive effects. First, it allows customers to capture some of the economic surplus that the provider can realise over the long-term relationship with a customer who faces switching costs after the adoption of the service. Second, discounts can offset parts of customers' switching costs and can thus encourage switching between providers. Third, cloud credits can motivate customers to sample new services which may lead to increased adoption of innovation.

In contrast, there have been concerns that cloud credits could also have anti-competitive effects.[177] In the context of additional switching costs for customers, Autorité de la concurrence fears that hyperscalers could use cloud credits to an extent that is not replicable by smaller competitors, and thus gain a long-term competitive advantage.[178] This sentiment is echoed by some cloud providers (that compete with hyperscalers) who state that they cannot match the long-term credits offered by hyperscalers (that have "deep pockets").[179] However, substantial benefits for customers should also be the outcome of effective ex-ante competition when customers are expected to remain in a long-term relationship with a specific vendor. Moreover, the expected stream of long-term profits should also provide smaller cloud providers with opportunities to finance ex-ante benefits and discounts for customers[180], even though it may be more difficult for them to diversify the risk of start-up

[171] Ofcom, 2023, p. 58 (n 6).
[172] Autorité de la concurrence, 2023 (n 5).
[173] Ibid.
[174] Ofcom, 2023 (n 6).
[175] Ofcom, 2023, p.58 (n 6).
[176] Farrell & Klemperer, 2007 (n 115).
[177] Autorité de la concurrence, 2023 (n 5).
[178] Ibid.
[179] See Ofcom, 2023, p. 163 (n 6).
[180] See also ACM, 2022, p. 46 (n 5) on cloud credit offers by cloud providers other than the hyperscalers.

bankruptcy[181]. Finally, a further tentative concern has been raised with respect to targeted cloud credits that may be used by cloud service providers to steer customers towards their own proprietary services and away from competing services of ISVs that are available in the provider's ecosystem.[182]

Committed spend discounts

Alongside cloud credits, many cloud providers offer committed spend discounts that provide customers with a percentage reduction in price in return for their agreement to spend a set amount with the provider.[183] Committed spend discounts may relate to individual services, families of services, or a customer's total spend with a cloud provider.[184] In general, it holds that "the more a customer spends on the provider's cloud services, the greater the discount received".[185] Again, such pricing discounts in return for longer-term customer commitment can be seen as a reflection of the typical pricing pattern in markets where customers face switching costs after adopting a vendor and extract some of the economic surplus of this relationship ex-ante.[186] In addition, longer-term contracts and spending commitments offer cloud providers greater certainty about customer demand and corresponding planning of capacity investments. The associated cost savings may then be (partially) passed on to customers through committed spend discounts.[187] Additionally, cloud providers may offer "spot pricing discounts" to efficiently allocate demand to under-utilised resources.[188]

According to Ofcom's market study, customers' perception in the UK differs with respect to their ability to negotiate the terms of a cloud contract. Some customers see no or only limited possibilities to negotiate with hyperscalers, even in the case of larger companies, which they attribute to their increasing dependence on their cloud provider.[189] In contrast, a greater number of customers stated that they could negotiate discounts if they were willing to commit to longer contract length and higher committed spend.[190]

From the perspective of a customer, committed spend discounts can give rise to economies of scope, as provisioning services from a single cloud provider becomes less costly relative to provisioning services from different cloud providers. In this vein, committed spend discounts can discourage the adoption of multi-cloud approaches by increasing the opportunity costs for replacing a single service with a service by a different provider.[191] In turn, switching costs of the customer for the overall ensemble of services are likely to increase when all services are provisioned from a single cloud provider (for instance, due to the need for compatibility across services). Similar concerns may apply

[181] ACM, 2022 (n 5); Ofcom, 2023 (n 6).
[182] Ofcom, 2023, p. 164f. (n 6).
[183] Ofcom, 2023 (n 6).
[184] Ibid.
[185] Ibid, p. 7.
[186] Farrell & Klemperer, 2007 (n 115).
[187] Ofcom, 2023, p.58 (n 6).
[188] Ibid.
[189] Ibid, p. 49.
[190] Ibid.
[191] Ofcom, 2023 (n 6).

to other pricing models, where customers receive a discount for buying several services from the same provider.[192]

At the same time, committed spend discounts, which basically resemble general quantity discounts, are a common pricing instrument in many industries. In this vein, they represent a direct benefit to customers and can have pro-competitive effects as mentioned for cloud credits with respect to giving customers the ability to extract economic value from long-term relationships and their potential to (partially) offset customers' switching costs. As customers make strategic adoption decisions, they can be expected to weigh the benefits and costs of committing to spend a set amount at a specific cloud provider and to search for the most attractive ex-ante offer across cloud providers. Moreover, the majority of committed spend discounts seem to include no exclusivity obligation (on the competitive implications of such contracts).[193] Hence, customers maintain the (contractual) flexibility to provision services from other cloud service providers even after they have agreed to committed spend discounts. Furthermore, the employed pricing schemes seem not to stipulate any requirement on the share of a customer's overall cloud spend or take-up of competing cloud services as is common for loyalty rebates.[194]

4.1.5 Summary

Although customers face switching costs in many markets, cloud computing services exhibit several peculiar types of switching costs. As summarised above, these switching costs can arise from technical and financial barriers to switching. Therefore, the possibility and extent of vendor lock-in in cloud computing are determined by the interplay of these different types of switching costs and, ultimately, the sum of switching costs that accumulates for customers. When assessing the competitive implications of switching costs, it is important to consider customers as strategic actors and the extent of their ability in specific markets to negotiate ex-ante benefits that can compensate for higher long-term costs due to the presence of switching costs. In general, we consider that data-induced switching costs, technical incompatibility, and data egress fees can together constitute significant costs for switching and may give rise to vendor lock-in for certain types of customers and services. The Data Act introduces a range of important provisions that directly target these types of switching costs and aim to reduce potential vendor lock-in (see Section 3.2). In Section 5, we analyse the economic trade-offs involved with these specific regulatory approaches, which provides the basis for our recommendations in Section 6.

Whereas committed spend discounts can add to the switching costs of customers, these and similar practices (like cloud credits) are associated with direct (often short-term) benefits for customers. Hence, these practices are in line with the expected outcomes of markets with switching costs, where cloud providers compete for customers by offering ex-ante benefits. Therefore, upfront discounts and associated practices should be treated with particular caution in case of possible regulatory intervention, as these practices can have pro-competitive effects and intervention may result in adverse effects for customers. With respect to interoperability, our analysis highlights that, in the

[192] See ibid, p. 49.
[193] Ide, E., Montero, J. P., & Figueroa, N. (2016). Discounts as a Barrier to Entry. *American Economic Review*, *106*(7), 1849-1877.
[194] See Calzolari, G., & Denicolò, V. (2020). Loyalty discounts and price-cost tests. *International journal of industrial organization*, *73*, 102589; Scott Morton, F. M., & Abrahamson, Z. (2016). A unifying analytical framework for loyalty rebates. *Antitrust LJ*, *81*, 777.

context of vendor lock-in, interoperability may not be seen so much as an ultimate and universal end in itself (although interoperability may have broader benefits), but as a means to decrease switching costs from technical incompatibility and to provide customers with a credible technical threat of switching through the ability to establish multi-cloud approaches (see also Section 5.5). The implementation of the Data Act and specifically the provisions in Chapter VIII stipulate important provisions in this regard (see Sections 3.2.2 and 3.2.7). In general, our analysis highlights that the identified types of switching costs can often result from a range of different motives of cloud service providers and have manifold economic effects. We discuss the resulting trade-offs with respect to these issues in our analysis of regulatory approaches in Section 5.

4.2 Economies of Scale and Scope

Next, we analyse economies of scale and scope with respect to their impact on competition in the cloud computing industry. Whereas economies of scale and scope do not constitute market failures per se, and can in fact also be important sources for welfare gains, they have a significant impact on competition and can lead to competition concerns. Before we analyse the role of economies of scale and scope in the specific context of cloud computing, the general competition effects and economic trade-offs associated with scale and scope advantages are summarised first.

In general, economies of scale promote market concentration, as larger firms have an efficiency advantage over smaller firms. Such concentration is beneficial from a productive efficiency perspective, as firms need to operate at a larger scale to minimise the total costs of production. In contrast, from an allocative efficiency perspective, market concentration can lead to inefficient outcomes as market concentration facilitates price increases by larger firms. In general, economies of scale therefore give rise to a welfare trade-off between the cost savings from scale on the one hand and price increases from market concentration on the other hand. Next to this central trade-off, it is important to consider the possibility of market entry when evaluating the competitiveness of markets characterised by economies of scale. The threat of entry can constrain incumbents' ability to raise prices and market entry plays an important role in generating innovations over the long run. To this end, entrants have to overcome market entry barriers from scale advantages, as they frequently operate at a lower cost efficiency than incumbents at the time of entry.

Economies of scope augment scale advantages beyond an individual product market, as they provide integrated firms with a cost advantage when producing different goods over specialised firms that focus on the production of a single competing product. Similar to economies of scale, economies of scope therefore yield efficiency advantages that can be beneficial for total welfare and customers. However, the emergence of integrated service ecosystems spanning across individual markets can also increase market entry barriers to individual markets. In consequence, this can raise concerns about competition intensity within these markets and the ability of specialised firms to innovate in individual product markets. If scope advantages are strong, competition between firms may not play out independently in each individual product market but between the offers of integrated ecosystems as customers decide about the purchase of a bundle of dependent products.

4.2.1 Economies of scale and scope in cloud computing

Cloud computing is characterised by significant economies of scale.[195] This means that average costs are decreasing in the scale of a provider's operations and, in consequence, a firm with more output can operate at lower average costs than a firm with less output. Economies of scale are at the heart of cloud computing's value proposition, as scale efficiencies are a key driver of the lower prices for computing resources. This cost advantage represents one of the main motivations of customers to adopt cloud services (see Section 2.2).

Economies of scale arise especially at the IaaS layer. First, this is due to the need for large investments into physical infrastructures that entail significant fixed costs. This applies especially to data centres, which house computing and storage servers, and network infrastructure that are both crucial to providing IaaS services. For fixed-cost investments, the average costs per unit of output decline with increasing utilisation. Second, operating costs of cloud computing services also decrease with larger scale.[196] In particular, data centres of larger size can operate at significantly lower average energy costs, which account for a large share of the total costs of a data centre [197] Third, the provision and utilisation of shared resources, a core characteristic of data processing services, implies scale advantages. A larger firm can utilise its shared infrastructure more efficiently, as the demand for this infrastructure balances across customers. The larger the number of customers, the less idle capacity needs to be reserved in relative terms of the entire shared infrastructure, thus leading to lower average costs per unit of output. Fourth, and related to the previous point, multi-tenancy lowers the maintenance costs per customer as the infrastructure and computing resources that must be operated and managed by the cloud provider are less fragmented and differentiated.[198] Fifth, and more generally for cloud services of the entire cloud computing stack, quality-of-service features such as security and reliability can feature economies of scale. These features are often established, developed or purchased at a fixed cost, which can then be spread over the entire output, thus yielding decreasing average costs per unit of output.

Cloud computing also features significant economies of scope.[199] First and foremost, the same IT infrastructure can be used to offer a variety of different cloud services. By deploying different services on a shared infrastructure, an integrated cloud provider can gain cost advantages over independent providers of stand-alone services by more efficiently utilising the underlying infrastructure. Utilising an existing IT infrastructure to develop new services can further save fixed costs and lump-sum investments that must be incurred by a stand-alone provider of the same service. The importance of these synergies is illustrated by the fact that hyperscalers as well as many other IaaS cloud service providers have developed their cloud businesses by utilising and expanding the IT infrastructure

[195] See also Schnurr, 2023 (n 17).
[196] ACM, 2022 (n 5).
[197] ACM, 2022 (n 5); Microsoft (2010). The Economics of the Cloud. https://news.microsoft.com/download/archived/presskits/cloud/docs/The-Economics-of-the-Cloud.pdf; Banet, Pollitt, Covatariu & Duma (2021). Data Centres and the Grid – Greening ICT in Europe. CERRE Report. https://cerre.eu/publications/data-centres-and-the-energy-grid/
[198] Microsoft, 2010 (n 198).
[199] See also Schnurr, 2023 (n 17).

originally established for the operations of their core business units.[200] In this vein, these cloud providers still benefit from cost synergies between their cloud and non-cloud services.[201] In addition, these cloud providers may also incur lower costs for marketing and advertising their services to customers than stand-alone providers, as they can leverage direct access to customers of their non-cloud services.[202] Economies of scope can further arise from skilled human resources and technical expertise, which represent important inputs for developing cloud services. These skills and expertise are subject to significant learning effects. In consequence, established cloud providers with a broad developer base will have significant advantages over stand-alone service providers. These synergies arise particularly for similar cloud services at the same layer of the cloud stack, which share similar features and code bases, but may also extend to cross-layer skills such as for cloud security. Finally, learning effects may not only occur at the individual level but also at the organisational level. Thus, access to large data sets from customer interactions and their usage of services may provide integrated cloud providers with an advantage over stand-alone and smaller providers when developing, updating, or advertising services.[203]

4.2.2 Integrated cloud service ecosystems, network effects, cloud marketplaces and ISVs

Integrated cloud service ecosystems

Alongside these economies of scope, there are also technical benefits from integration, compatibility, and tight coupling of cloud services. Whereas loose coupling of services and interconnection of incompatible services can be achieved by APIs, common ontologies, and additional abstraction layers, services built on a common technological basis and a shared overarching architecture can often achieve better overall performance and a lower risk of errors for workloads that require the interplay of several services. This is not to say that modularisation and decoupling do not entail significant technical benefits over monolithic services, as illustrated by the success of microservices architectures.[204] But even for those architectures, dependencies among services and modules are more easily managed in an integrated environment. In fact, increasing modularisation increases the need for cross-cutting coordination, integration and management of individual services such that interoperability, performance, and high quality of service ensembles can be maintained. Such coordination and integration can often be achieved at lower transaction costs within the boundaries of a single organisation (including both ex-ante costs from coordination as well as ex-post costs from hold-up).

Furthermore, some customers may value integrated offers of broad service bundles as this reduces the complexity of their IT infrastructure as well as their business relationships. In consequence, a 'one-stop shop' for different types of services can lower the transaction costs of provisioning cloud services for customers. For example, among IaaS and PaaS customers in the UK, 31% of customers rated the 'number of features' as an important factor when choosing a cloud provider.[205] Of course, customers' valuation of integration is to some extent an endogenous consequence of the cloud service providers'

[200] See, for example, Miller (2016). How AWS came to be. https://techcrunch.com/2016/07/02/andy-jassys-brief-history-of-the-genesis-of-aws/
[201] Ofcom, 2023, p. 146 (n 6)
[202] Autorité de la concurrence, 2023 (n 5).
[203] See also ibid.
[204] Sill, A. (2016). The design and architecture of microservices. *IEEE Cloud Computing*, *3*(5), 76-80.
[205] Ofcom, 2023, p. 52 (n 6).

choice of technical compatibility (as discussed in Section 4.1), but may nonetheless reflect additional benefits from integrated service offers as discussed above. In general, these benefits give rise to economies of scale from the perspective of customers, who then have to weigh such benefits against potential downsides from increased switching costs (see also Section 4.1).

In consequence, these cost and demand characteristics of cloud services promote the emergence of *integrated cloud ecosystems*, as demonstrated by the broad range of service offerings of hyperscalers. As noted above, this can shift the focus of competition to a customer's decision for an entire bundle of services and the associated choice for a specific cloud ecosystem. In consequence, smaller and more specialised providers may then find it more difficult to attract customers, as they cannot offer the same breadth of services. Moreover, they may even find themselves at a competitive disadvantage in their core markets, as they cannot benefit from the same economies of scale and scope as large and integrated providers. At the same time, smaller service providers may benefit from advantages over larger firms because of their specialised services that target the peculiar requirements of an industry or a customer segment. They may also provide services that require more extensive human resources, which is subject to lesser scale economies than computing resources (see, for instance, Quinn, 2020 for anecdotal examples).[206] Large-scale technical implementations are also more difficult to change, which can give smaller competitors an advantage when organisations must adjust existing solutions or adapt to new circumstances. Overall, this suggests that smaller firms may be able to compete successfully in smaller niche markets by providing specialised services. In this context, the expected imminent rise of edge computing, which frequently requires more customisation and tailoring of services to industry-specific needs, could present a significant growth opportunity for more specialised providers.[207] However, for mainstream services, especially at the IaaS layer, economies of scale and scope are likely to give larger providers that offer integrated ecosystems a sustained competitive advantage over smaller competitors.

Network effects, cloud marketplaces and ISVs

With respect to market characteristics, it is important to note that compared to other digital platform services, the cloud computing industry today does not feature the same multi-sided market structure and therefore does not exhibit significant cross-sided network effects with the exception of cloud marketplaces. Nonetheless, indirect network effects still exist in cloud computing markets. For example, the more customers use a cloud service, the more customers will be available to buy complementary resources, such as consulting services or public knowledge resources.[208] However, these more limited network effects are common in many other industries and are generally weaker than the cross-sided network effects in digital platform markets, where service providers act as intermediaries between different market sides (such as online marketplaces or app stores).

The exceptions are cloud marketplaces that are offered by hyperscalers, among others, and allow customers to purchase the cloud providers' own services but also services of third parties such as ISVs

[206] Quinn (2020). How to compete with AWS. https://www.lastweekinaws.com/blog/how-to-compete-with-aws/
[207] European Commission (2022). IoT and the Future of Edge Computing in Europe. https://digital-strategy.ec.europa.eu/en/news/iot-and-future-edge-computing-europe
[208] Katz, M. L., & Shapiro, C. (1985). Network externalities, competition, and compatibility. *The American Economic Review*, *75*(3), 424-440.

(see Section 2.2). These cloud marketplaces represent genuine two-sided markets, where the cloud provider acts as an intermediary between customers and cloud service providers.[209] Therefore, they feature positive cross-sided network effects, as ISVs have a greater incentive to be available on a marketplace of cloud providers with a larger number of customers, and vice versa. Thus, ISVs have also an incentive to provide a customised version of their service within the cloud provider's ecosystem that can be easily integrated with other services in the ecosystem. In consequence, cloud marketplaces could further promote the emergence and consolidation of integrated cloud service ecosystems, as cross-sided network effects add demand-side economies of scale and facilitate market concentration.[210] However, at least for IaaS and PaaS services in the UK, customer's use of marketplaces for provisioning ISVs seems to be limited so far. As cited in Section 2.2, only 13% of all customers surveyed by Ofcom mentioned that they were buying third-party services through the hyperscalers' marketplaces, although, 51% of respondents indicated that they were using marketplaces for some purpose.[211]

Ecosystem competition and market concentration at the IaaS layer as a consequence of economies of scale and scope raise the question of how effectively ISVs can compete with integrated hyperscalers at the PaaS and SaaS layers.[212] Whereas some of these ISVs may be able to provision their infrastructure independently and compete with hyperscalers' PaaS and SaaS layers outside of their ecosystem, others may rely on the hyperscalers' IaaS services and join the ecosystem of a cloud provider as a third-party 'partner service'.[213] Being part of a hyperscaler's ecosystem can provide ISVs with the advantages of higher visibility to customers and easier interconnection with other services of the hyperscaler. This requires that the ISV has access to the hyperscaler's services and its ecosystem. If an ISV and a hyperscaler also compete in specific PaaS and SaaS markets, such access relationships can raise concerns about the hyperscalers' ability to steer demand to its proprietary services or to raise the costs of its competitors.[214] However, by providing a complementary service that increases the value of the ecosystem to customers, there is also an inherent economic incentive for the hyperscalers to attract these partner services and offer them to customers. In this vein, the relationship between ISVs and hyperscalers resembles other digital markets where independent complementors and ecosystem providers compete and collaborate at the same time, while different ecosystems compete for customers.[215]

[209] Parker, G. G., & Van Alstyne, M. W. (2005). Two-sided network effects: A theory of information product design. *Management Science*, *51*(10), 1494-1504 ; Armstrong, M. (2006). Competition in two-sided markets. *The RAND journal of economics*, *37*(3), 668-691;

[210] Evans, D. S., & Schmalensee, R. (2007). Industrial Organization of Markets with Two-Sided Platforms. *Competition Policy International*, *3*(1), 151-179; Furman J, Coyle D, Fletcher A, McAules D and Marsden P (2019) Unlocking digital competition. Report of the Digital Competition Expert Panel for the Government of the United Kingdom, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf

[211] Ofcom, 2023 (n 6).

[212] See, e.g., Ofcom, 2023 (n 6).

[213] See, e.g., AWS (2023). AWS ISV Accelerate. https://aws.amazon.com/de/partners/programs/isv-accelerate/

[214] Cf. Autorité de la concurrence, 2023 (n 5).

[215] Foerderer, J., Kude, T., Mithas, S., & Heinzl, A. (2018). Does platform owner's entry crowd out innovation? Evidence from Google photos. *Information Systems Research*, *29*(2), 444-460 ; Zhu, F., & Liu, Q. (2018). Competing with complementors: An empirical look at Amazon. com. *Strategic management journal*, *39*(10), 2618-2642 ; Adner, R., Chen, J., & Zhu, F. (2020). Frenemies in platform markets: Heterogeneous profit foci as drivers of compatibility decisions. *Management Science*, *66*(6), 2432-2451.

4.2.3 Summary

Economies of scale are a key characteristic of the cloud computing industry, especially at the IaaS layer. In general, these scale advantages facilitate market concentration when not offset by benefits of specialisation. In consequence, one can expect that the mainstream of IaaS services will be provided by a smaller number of large providers due to the importance of economies of scale as the industry matures. As discussed above, on the one hand, the resulting market concentration can soften competition intensity and lead to prices above the efficient welfare level, which can give rise to market failure. On the other hand, a concentrated market structure reflects the underlying cost structure and allows providers to exploit the scale and scope efficiencies, which can also benefit customers if these efficiencies are passed on through lower prices.

Economies of scale make profitable entry and large-scale growth other than in niche markets difficult at the IaaS layer. Nonetheless, there are currently indications of competition between cloud providers of different sizes[216], although a large share of the markets, including the take-up of new customers, is captured by hyperscalers.[217] As the focus of competition is currently on new customers that migrate to the cloud for the first time, there remain concerns that switching costs and the resulting vendor lock-in (see Section 4.1) could lead to less competition at the IaaS layer over the long run, especially for mainstream services. However, with respect to the current market situation, market research suggests that there is evidence of at least some customers switching between providers, as "18% of customers switched IaaS/PaaS providers" in the UK according to Ofcom.[218]

Compared to the IaaS layer, market entry at the PaaS layer and especially at the SaaS layer is significantly easier from a cost perspective, as application developers and service providers can make use of cloud infrastructure services themselves. In this vein, IaaS services have facilitated the entry and growth of many SaaS offerings, thus having positive effects on competition and innovation. However, by relying on IaaS services, PaaS and SaaS service providers can become more dependent on hyperscalers, as the major providers of these underlying services. This could raise concerns over the long term if IaaS services become further concentrated and technical and financial switching costs complicate switching IaaS providers for ISVs.

Furthermore, independent PaaS and SaaS service providers may compete with the same hyperscalers that they also rely on with respect to access to IaaS services. In general, this can raise concerns about a level competitive playing field, especially for PaaS services where the differentiation and diversity of services are more limited and thus independent providers are likely to compete head-to-head with vertically integrated providers for the same customers (see, for instance, MongoDB vs. AWS DocumentDB vs. Azure Cosmos DB).[219] At the same time, hyperscalers have an incentive to partner with ISVs and support these services as part of their broader ecosystem offers, when the services of ISVs are valued by customers. In this vein, the relationship between ISVs and hyperscalers resembles other digital markets where independent complementors and ecosystem providers compete and

[216] ACM, 2022 (n 5); Ofcom, 2023 (n 6).
[217] Autorité de la concurrence, 2023 (n 5).
[218] Ofcom, 2023, p.94 (n 6).
[219] Ittycheria, D. (2019). The Future Will Be Documented. https://www.mongodb.com/blog/post/the-future-will-be-documented; Nehme, R. (2017). Dear DocumentDB customers, welcome to Azure Cosmos DB! https://azure.microsoft.com/de-de/blog/dear-documentdb-customers-welcome-to-azure-cosmos-db/

collaborate at the same time. At the SaaS layer direct competition between independent and vertically integrated cloud service providers occurs less often because of greater opportunities for service differentiation and specialised markets. Nonetheless, there exist specific service markets where such direct competition between ISVs and integrated cloud service providers takes place.

Even if ISVs do not rely on the IaaS services of their competitors, integrated cloud providers frequently have a competitive advantage over ISVs due to their ability to offer broad service ecosystems. Economies of scope and technical benefits from integration facilitate the emergence of these service ecosystems offered by a small number of cloud service providers. In turn, this can increase entry barriers for smaller and more specialised cloud providers. However, customers also benefit from integrated services and scope efficiencies and, to some extent, internalise the trade-off between more integration and more openness when choosing between cloud services and deciding about their overall architecture of provisioned services.

As the cost and demand characteristics of cloud service markets give rise to the general trade-off between efficiencies from large-scale and integrated ecosystems, on the one hand, and more concentrated markets, on the other hand, the general focus of regulation and competition policy should be on (i) monitoring the ability of ISVs to enter and compete in their specific services markets and (ii) safeguarding and promoting competition intensity by reducing switching costs that could promote the lock-in of customers (see Section 4.1).

5. REGULATORY APPROACHES AND ASSOCIATED TRADE-OFFS

Recent policy interventions at the EU level, as discussed in Section 3, have stipulated a set of new rules for cloud computing services. In the context of ongoing investigations at the national level, further measures and interventions are currently being debated. In this section, we evaluate selected regulatory measures and policy options in light of the competition issues analysed in Section 4 and discuss the associated economic trade-offs of these regulatory measures.

5.1 Data Portability

Data-induced switching costs are peculiar switching costs of cloud computing services that can contribute to vendor lock-in.[220] Both the Data Act (under Article 23 I and Article 30 (5)) and the Digital Markets Act (under Article 6 (9) and (10)) stipulate data portability rules, which shall allow customers to export their data at the original service provider in order to be able to transfer this data to the destination service provider.

In general, data portability rules have to specify the scope of data, the mode of portability, and possible conditions on the data format. To facilitate switching, the scope of data should generally include all of the customer's data, that is, the data that the customer has initially imported and the data that the customer has generated during the use of the service.[221] This is usually straightforward in the case of IaaS and PaaS services but more complex in the case of SaaS services, as data created during the customer's usage of SaaS services is often heterogeneous and stored in proprietary formats. In the case of IaaS and PaaS services, the inclusion of customer-generated metadata such as the configuration of settings and virtual machines can lower transaction costs for a switching customer, but this data may also often exist only in proprietary data formats.

With respect to the mode of portability, data may be exportable manually by a download function or continuously and in real-time through the support of APIs. Manual export functions are usually sufficient to support a customer in switching cloud providers, as the data basis has to be replicated once at the destination service provider.[222] In contrast, continuous and real-time data portability can support the parallel use of services of the same service type at different service providers, as it allows for the continuous synchronisation of the underlying data basis. However, such multi-homing use cases seem not very common among customers[223] and remain relatively complex from a technical perspective even if continuous, real-time data transfer is feasible.

Data portability can only effectively reduce customers' switching costs if the exported data can be imported and processed by the destination service provider. To this end, the data should be in a structured, commonly used, non-proprietary, and machine-readable format. This ensures that the

[220] Wohlfarth, 2019 (n 129); Arce, 2022 (n 114).
[221] Making a distinction between customer-created and provider-created metadata, which the Data Act does not (see Section 3.2.5), can help to protect the legitimate business interests of the involved parties. However, protection of intellectual property or trade secrets should not unduly restrict customers in their ability to switch (see also Schnurr, 2023, (n 17)).
[222] Schnurr, 2023 (n 17).
[223] Autorité de la concurrence, 2023 (n 5).

destination service provider or the customer (or third parties on its behalf) can read the ported data and extract information. There remains a risk that even such general criteria could negatively affect innovative activities if cloud service providers would prefer to develop services based on new proprietary and possibly niche data formats, which would then need to be converted on the request of the customer.

Even if data is stored in an easily portable format, this does not necessarily mean that the data can be readily imported without further need for data processing, as the semantics of the data are usually not immediately available from the ported data unless the destination service provider offers the same service as the original service provider (such as an open-source platform or application). Therefore, although data stored in proprietary formats at the original service provider can usually be converted into open data formats, unclear semantics are likely to present challenges for immediately importing such data at the destination service provider. Similar semantics-related challenges have been experienced in other domains of IT, most prominently in the context of the "Semantic Web".[224] Although there exist several technical approaches to establish a common understanding of data semantics (such as domain specific languages and ontologies), these approaches have so far failed to achieve widespread adoption in contexts such as the World Wide Web with a large service heterogeneity, distributed architectures, and a large number of stakeholders.[225]

In the context of data portability for end users, incompatibilities between data formats have been identified as a main impediment to the effectiveness of data portability.[226] However, standardisation of uniform data formats for data portability among cloud providers is difficult to realise from a technical perspective due to the differentiated features and heterogeneous technical implementations of cloud services. Next to the complexity of establishing a common standard that would satisfy the requirements of most providers, standardisation is further complicated by the constant evolution of existing services and the introduction of new cloud services. Thus, the challenges and costs associated with establishing uniform standards for data are generally very high. There are two more specific areas, where standardisation of data portability formats may nonetheless be considered, even though the potential detrimental effects of standardisation on providers' constrained flexibility and on competitors' more limited ability to differentiate themselves need to be taken into account.

Compared to other layers of the cloud stack, the complexity of establishing a common standard for data portability (especially for selected types of metadata) will most likely be the lowest at the IaaS layer (although complexity can still be very significant due to the aforementioned reasons), where cloud services are more homogenous than at other layers of the cloud stack with respect to their feature set.[227] However, even at the IaaS layer, services with similar features may be based on different

[224] Ranabahu, A., & Sheth, A. (2010). Semantics centric solutions for application and data portability in cloud computing. In *2010 IEEE Second International Conference on Cloud Computing Technology and Science* (pp. 234-241). IEEE.

[225] Cf. Fournier-Viger, P. (2018). The Semantic Web and why it failed. https://data-mining.philippe-fournier-viger.com/the-semantic-web-and-why-it-failed/

[226] Krämer, J. (2021). Personal data portability in the platform economy: economic implications and policy recommendations. *Journal of Competition Law & Economics*, *17*(2), 263-308 ; Syrmoudis, E., Mager, S., Kuebler-Wachendorff, S., Pizzinini, P., Grossklags, J., & Kranz, J. (2021). Data Portability between Online Services: An Empirical Analysis on the Effectiveness of GDPR Art. 20. *Proc. Priv. Enhancing Technol.*, *2021*(3), 351-372.

[227] Cf. ACM, 2022, p. 51 (n 5).

technological solutions and provide customers with significant variations in functionality. At the SaaS layer, the diversity of different service types will make it generally very challenging to establish a consensus on a common data format across providers. However, standardisation of data formats could be considered as a regulatory option in specific service markets that feature a high market concentration. In such markets, the pro-competitive benefits from a standardised data format due to lower switching costs can be expected to be relatively high. In addition, such markets will involve a smaller number of service providers, which can reduce the complexity of establishing a common standard.

Even if no standardised data format is available, data portability can still facilitate the switching of cloud providers. In contrast to end users, which were the focal point of other data portability regulations such as in the GDPR, business customers have greater capabilities for and larger expected benefits from extracting relevant information from extracted data and possibly converting data into compatible formats themselves. Moreover, destination service providers have an incentive to provide tools and support for data migration (see also Section 4.1), which can facilitate data import once the data can be exported from the original service provider. Hence, data portability has the potential to reduce customers' switching costs even if the data may not be directly importable. Such data portability regulation still entails implementation costs for cloud service providers and regulatory costs in terms of oversight and enforcement. However, in total, these costs are much lower than those for establishing and enforcing an industry-wide standardisation of data formats for cloud computing in general.

To protect the legitimate interests of cloud service providers, data portability regulation should typically be limited to customer-created data and include exceptions for data that could reveal business secrets or information protected by intellectual property rights. However, in order to ensure the effectiveness of data portability rules, the cloud provider should be able to exclude such information only on an exceptional basis and bear the burden of proof for demonstrating this. Similar exceptions may be included to protect the data of third parties or data related to the integrity and security of the service (cf. Section 3.2.5 on data portability exceptions in the Data Act).

Data portability: Key trade-offs and considerations

Data portability can lower switching costs by reducing technical barriers to switching. This comes at implementation costs for cloud service providers and regulatory costs for oversight and enforcement.

Standardisation of data formats can further decrease data-induced switching costs but is complex and costly to achieve through mandatory regulation in the context of heterogeneous, differentiated, and continuously evolving cloud services. In particular, mandatory standardisation entails the risk of impeding innovation by restricting the data formats that service providers can use to develop new services or features. Mandatory standardisation of data formats may thus be limited to selected cases, where services are rather homogeneous, markets are concentrated data

portability is of high value to customers. In general, portable data should be made available in a structured, commonly used, open, and machine-readable format.

One-off data portability is sufficient for many cases of customers switching providers, whereas continuous data portability facilitates interconnection and thus multi-cloud approaches.

5.2 Application Portability

Compared to data portability, application portability, that is, the ability of customers to move services between ecosystems of cloud providers without further modifications, could further reduce customers switching costs by lowering technical barriers to switching. However, application portability is associated with significant technical challenges due to the diversity and heterogeneity of cloud services across service providers (see also Section 4.1).

Application portability requires vertical interoperability with the underlying layer(s) of cloud services as well as with native management functions of a cloud provider's environment (for instance, for authentication, billing, or monitoring). Both can result in strong dependencies between a cloud service and the corresponding provider.[228] With respect to the cloud management functions, each cloud service provider has usually its particular APIs, configuration tools, and restrictions. With respect to the underlying service functionalities, a service requires access to service-specific interfaces and functions (such as those of the supporting IaaS services) and must be able to exchange data with these underlying services in a compatible and meaningful format. For example, in the case of PaaS services, dependencies may arise from the required runtimes for programming languages, middleware, and software frameworks. To resolve these dependencies, there are, in principle, two technical approaches: either porting the application with its entire dependencies, that is, including all the necessary input services, or trying to map the dependencies onto the functions and interfaces offered by the destination service providers. Of course, the mapping of dependencies requires that the destination service offers the same (or at least very similar) functionalities and interfaces for its underlying services as the original service provider or the ability of the customer to develop support for these functions on its own.

From a technical perspective, moving an entire application with its dependencies is most feasible at the IaaS layer, as services are rather homogeneous in their feature set and often build on similar standard hardware and infrastructure inputs. However, some cloud providers may also develop their own hardware and infrastructure inputs or rely on specialised inputs of third parties. It has further been argued that standardisation of IaaS services would deliver the most immediate benefits to customers, as virtual machine images and storage units represent the main building blocks of customers applications, and as such could be moved between IaaS providers as self-contained software containers to others.[229] For such containers and virtual machine images, there currently exist

[228] Kolb & Wirtz, 2014 (n 21).

[229] Lewis, G. A. (2013). Role of standards in cloud-computing interoperability. In *Proceedings of the 46th Hawaii International Conference on System Sciences (HICCS)* (pp. 1652-1661). IEEE.

different proprietary and open-source solutions that are supported to some extent by cloud service providers and hyperscalers.[230] In addition, cloud service providers offer tools and documentation to support the migration of IaaS services across providers, although these procedures seem more reliant on data portability rather than representing genuine application portability.[231] However, despite several standardisation initiatives,[232] there is no common uniform standard across IaaS offerings. Hence, also at the IaaS layer, customers frequently have to undertake technical modifications and engineering efforts when porting services across providers, which raises their costs of switching.

At the PaaS level, porting an application with all its dependencies is technically even more difficult, as service features and implementations differ significantly across providers. As an alternative approach, application portability may thus be facilitated by the mapping of dependencies across providers, which can be achieved by the specification of machine-readable service profiles.[233] Such service profiles are intended to describe the core properties and corresponding dependencies of a cloud service. Based on this approach customers could identify whether application portability between two providers is readily feasible, or which dependencies would otherwise need to be resolved by additional implementation efforts. Technical challenges of such an approach include the establishment of a commonly used language to specify such service profiles as well as to keep service profiles accurate and up-to-date. In this vein, the envisioned Gaia-X architecture can be viewed as an initiative to establish a common meta-standard for self-descriptions of services and resources, which could facilitate the identification of compatible and interoperable services across cloud service providers.[234]

Increasing the transparency regarding technical dependencies between specific cloud services and their providers does, in general, not eliminate the need for technical modifications and engineering efforts by the customer. However, it can inform customers about the feasibility of application portability and assist them in making informed decisions when weighing short-term adoption benefits against the risk of vendor lock-in due to switching costs from a lack of application portability. In general, customers have at least some choice between open-source and more common service implementations that are likely to facilitate switching and proprietary service implementations that are more difficult to port to a different cloud service provider (see Section 4.1). Thereby, avoiding proprietary service implementations is not without costs for customers, as such services may offer a better performance and easier integration within the native ecosystem of the cloud service provider.

However, any regulatory intervention aimed at mandating an exclusive open-source standard for specific services to ensure application portability would entail the same costs for customers. Whereas such mandatory standardisation represents the most direct measure to achieve application portability, it is also associated with the greatest cost. In particular, such an intervention would

[230] See, e.g., AWS (n.d.) Importing a VM as an image using VM Import/Export. https://docs.aws.amazon.com/vm-import/latest/userguide/vmimport-image-import.html; See further the reference to "VMs running in VMware vSphere and Microsoft Hyper-V" in AWS (2022). Announcing Azure to AWS migration support in AWS Server Migration Service. https://aws.amazon.com/about-aws/whats-new/2019/04/announcing_azure_awsmigration_servermigrationservice/

[231] See, e.g., Microsoft (2023) Tutorial: Discover AWS instances with Azure Migrate: Discovery and assessment https://learn.microsoft.com/en-us/azure/migrate/tutorial-discover-aws; Microsoft (2023). Discover, assess, and migrate Amazon Web Services (AWS) VMs to Azure. https://learn.microsoft.com/en-us/azure/migrate/tutorial-migrate-aws-virtual-machines

[232] Kaur et al., 2017 (n 18).

[233] Kolb & Wirtz, 2014 (n 21).

[234] Gaia-X European Association for Data and Cloud AISBL (2022). Gaia-X Architecture Document - 22.10 Release. https://docs.gaia-x.eu/technical-committee/architecture-document/22.10/

magnify welfare losses in terms of limiting innovation and differentiation of cloud services compared to those of mandatory standardisation of data formats for the purpose of data portability (see Section 5.2). Even for customers, it seems unlikely that these costs will be outweighed by the benefits of improved application portability, especially when data portability regulation can establish a similar (although less effective) safeguard for ensuring that switching providers is technically feasible.

Instead of mandating standards, regulatory approaches towards application portability may thus focus on empowering customers to make informed and voluntary choices between open-source and proprietary offerings. To this end, market-driven interoperability initiatives and open-source solutions may be supported by public procurement and by facilitating cooperation initiatives between providers. To this extent, there should be clear guidelines on what activities are considered pro-competitive, as concerns about anti-competitive collaborations could have chilling effects on such initiatives.[235] Moreover, regulators and competition authorities may monitor the availability of open-source solutions at hyperscalers to achieve an accurate understanding of the available choices to customers. In this context, concerns about practices of cloud service providers that could make it more difficult for customers to adopt open-source services should be investigated.[236] With respect to such practices, the main challenge for authorities will be to weigh the anti-competitive effects of increased switching costs for customers against the pro-competitive effects of increased service differentiation and promotion of innovation.

Application portability: Key trade-offs and considerations

Compared to data portability, application portability can further reduce technical barriers to switching for customers. However, application portability is significantly more challenging to achieve from a technical perspective, as it requires interoperability of the portable service with underlying cloud services and native functions of a cloud provider's environment. The technical complexity for achieving application portability generally increases with higher layers of the cloud stack due to more complex dependencies.

Application portability can be promoted by standardisation and/or interoperability frameworks that increase the transparency of service dependencies across providers. Mandatory standardisation is most effective in achieving seamless data portability but entails higher welfare costs in terms of constraining innovation and service differentiation. Mandatory standards could also hurt customers by limiting availability and benefits from proprietary, integrated service offerings. Transparency initiatives and voluntary interoperability frameworks likely leave customers with some implementation effort to port their services. However, they preserve more freedom and flexibility for cloud providers and empower customers to make the decision between more interoperable and more integrated, proprietary service offerings.

[235] Autorité de la concurrence, 2023 (n 5).
[236] See Ofcom, 2023 (n 6).

5.3 Price Regulation of Data Egress Fees

Many cloud service providers charge for data flows across their networks, both where data is transferred within the network and out of their networks. Data transfers out of a provider's network arise both in the normal course of a customer's business (such as a video streaming company sending a movie to one of its users) and when a customer is looking to switch cloud service provider or interconnect services of different cloud service providers. The fees associated with such transfers, often referred to as data 'egress' fees, therefore form part of customers' cloud costs. In particular, data egress fees represent direct costs of customers when switching to a different provider and needing to port data from the original service to the destination service (see Section 4.1). Moreover, data egress fees form part of the costs of customer's multi-cloud approaches, especially when services have to exchange significant data across providers, which can indirectly increase the costs of switching (see also Section 4.1). In the case of switching providers these costs for the customer may be (partially) offset by financial benefits offered by the destination service provider. In addition, several providers set non-linear pricing schemes such that costs for customers may only arise above a certain data traffic threshold.

To lower customers' financial switching costs, price regulation (as now enacted by the Data Act, see Section 3.2.4) may directly intervene in the setting of data egress fees. To this end, price regulation may require that data egress fees do not exceed the costs for the transfer of data (as now stipulated by Art. 34 (2) DA for the case of multi-cloud approaches) or may even stipulate a zero price (as required by Art. 30 (4) DA for the case of switching providers; see also Section 3.2.4). Moreover, price regulation may be differentiated for egress fees that arise in the immediate context of a customer switching providers and the egress fees that arise for the general operations of a service.

Price regulation represents an interference with a cloud provider's general commercial freedom to set its prices independently and thus with its right to conduct a business. Therefore, from an economic perspective, such an intervention must be justified by pro-competitive effects from lowering customers' switching costs and mitigating any vendor lock-in (see Section 4.1). Moreover, these potential pro-competitive effects must be weighed against the side effects of price caps as well as cloud providers' need to recover their costs associated with transferring data.

A general zero-price regime for data egress fees would prohibit providers from recovering any of their costs for external data transfer through a direct price of these costs. Consequently, cloud providers would need to recover these costs by charging other fees that are not based on data transfer usage, such as from internal cross-subsidisation and possibly by raising general cloud service prices. If price regulation is enforced symmetrically for all cloud providers irrespective of size and market power, this may negatively affect smaller providers, as their ability to spread costs across services and customers is more limited. Moreover, a general zero-price regime would eliminate any price signal for the efficient allocation of data traffic. As costs for external data transfers commonly exceed costs for internal data transfers (for instance, due to the co-location of services from one provider in a single data centre), a zero price for egress fees can create socially inefficient incentives for customers for excessive external data transfers. Hence, a zero price encourages multi-vendor cloud approaches but possibly at an inefficient level and by preventing cloud service providers from recouping costs.

In contrast, cost-based price regulation of egress fees would allow cloud service providers to recoup the costs for data transfer and send a price signal for efficient traffic allocation to customers. However, as in other instances of cost-based price regulation, this raises more intricate questions on the cost standard and the calculation of costs. In particular, it has been argued that marginal costs of data traffic are close to zero, anyhow, whereas cloud providers argue that traffic costs must reflect fixed-cost infrastructure investments. These challenges of cost-based price regulation have led to complex implementations and long-running litigation in other industries, most notably the telecommunications industry.[237] For data egress fees in cloud computing, the cost basis may be more straightforward to determine, as transit prices of third-party providers could give an indication of the market price for external data transfer that can serve as a general proxy and benchmark for cost-based egress fees. Nonetheless, accurate cost-based pricing of data transfers may involve several complex challenges, as the cost of a given data transfer to a provider can depend on the specifics of the transfer (for example, time of day, amount of data, start and end location, as well as the quality and associated costs of the provider's network).

With respect to data egress fees in the specific case of a customer switching providers, cost-based price regulation can lower financial switching costs to some extent but does not fully eliminate these barriers to switching. However, if the underlying egress fees are transparent to the customer, these costs can be anticipated by a customer at the point of initial service adoption and will thus be part of the overall cost-benefit analysis in the first place (see Section 4.1.3 for a more elaborate discussion on this issue). Decreasing the switching costs of customers further by the means of a zero price runs the risk that the original cloud provider may bear a significant one-time financial loss if the customers transfer large volumes of data that indeed incur substantial costs for data transfer. As these costs cannot be recouped ex-post, cloud providers would have an incentive to raise general service prices ex-ante, which would lead to a distorted price structure and a negative impact on other customers as they would need to cross-subsidise these costs from (presumably larger and data-intensive) customers. If a zero price is imposed symmetrically on all cloud service providers, there is also the concern that the exit decision of a large and data-intensive customer could lead to significant business risks for smaller providers due to the possible high one-time cost for external data transfer. Even if they can cross-subsidise these costs by raising service prices ex-ante, smaller cloud providers will likely be at a disadvantage compared to larger providers, as they can spread the costs for external data transfers of switching customers only on a smaller customer base and thus will likely need to raise prices more than larger providers.

Price regulation of data egress fees: Key trade-offs and considerations

Price regulation of data egress fees can decrease the financial switching costs of customers and thus possibly mitigate vendor lock-in. Regulation may directly lower the costs of switching for customers that need to transfer large data volumes as well as more indirectly lower the switching

[237] Conversely, this implies that European telecommunications regulators have gained significant experience in access price regulation, although arguably for very different product markets.

costs that arise from barriers to multi-cloud approaches. This comes at the cost of interference with cloud providers' freedom to set prices and the danger of distorting price signals.

A zero-price regime for data egress fees fully eliminates data-related financial switching costs for customers but prohibits cloud service providers from directly recovering any of the costs for external data transfer, which creates socially inefficient incentives for providers and customers. If applied symmetrically, a zero-price regulation can disadvantage smaller cloud providers. Cost-based price regulation of data egress fees allows for cost recovery and efficient price signals but raises implementation challenges and costs for regulation. Transit prices may serve as a general proxy and market-driven benchmark for cost-based regulation of egress fees.

5.4 Regulation of Discounts and Cloud Credits

Committed spend discounts may encourage customers to provision cloud services from a single provider and may thereby raise costs for later switching due to the need to port entire service ensembles instead of single services across providers. Moreover, many cloud providers offer cloud credits to entice customers to migrate to their cloud services. This has raised concerns that cloud credits could give larger cloud service providers a competitive advantage over smaller providers, as the latter may not be able to match the discounts offered by larger providers.[238] This could facilitate concentration and lead to higher prices in the long run.

To address these concerns, competition or regulatory authorities could attempt to intervene in cloud providers' pricing practices by limiting required commitments from customers, constraining the pricing schemes of providers, or outright banning such practices. Alternatively, non-discrimination obligations could be proposed to prohibit the targeting of discounts to specific groups of eligible customers. As discounts are frequently targeted to new customers, such a non-discrimination obligation may aim to make discounts more widely available for existing customers, thus lowering prices for a larger group of customers. Proponents of a ban on up-front discounts may argue along the same lines that competition should drive down general prices without the need for discounts, and, hence a ban, rather than time-limited and targeted benefits, could benefit a wider audience of customers.

However, these interventions run the significant risk that they could reduce or eliminate direct (often short-term) benefits for customers. In particular, if some structural switching costs persist, which is likely for the cloud computing industry due to its economic and technological characteristics (see Section 4), customers can be harmed by interventions that would reduce the ex-ante benefits of customers at the time of service adoption. In this context, it is important to recognise that upfront discounts are in line with the expected economics of markets with switching costs. For customers to benefit from competition in these markets, it is necessary that the competitive process can drive down prices at the time of adoption when customers can still more easily threaten to switch providers.

[238] Cf. Autorité de la concurrence, 2023 (n. 5).

Limiting or eliminating pricing instruments of providers, especially up-front discounts, therefore runs the risk of softening ex-ante competition.

Non-discrimination obligations can in principle lead to better offers for existing customers, as providers are then not able to differentiate their pricing between new and existing customers and thus may choose a compromise between higher prices for existing customers and lower prices for new customers.[239] However, this comes at the cost of new customers and their ability to negotiate favourable deals, while the overall net benefit for all customers is not clear. Moreover, discounts to small firms and especially startup firms may have particular welfare benefits, because such discounts lower the upfront costs and market entry barriers for businesses that are expected to promote overall innovation in the long term. Of course, cloud providers may look to appropriate some of this economic surplus over the long-term relationship with these customers, but the associated strategies to entice these customers through lower ex-ante prices can nonetheless be expected to create broader innovation benefits from a welfare perspective, as they benefit particularly innovative firms and can lower entry barriers for new and growing firms.

Finally, while committed spend discounts can reinforce customers' incentives to refrain from a multi-cloud approach, they can be the basis for mutually beneficial agreements between a cloud provider and a customer. In particular, a commitment by the customer to use a certain volume of a provider's services in exchange for price discounts can reduce demand uncertainty for the cloud provider and thus facilitate investments into hardware and computing capacity. Disallowing such agreements could thus hurt both the cloud provider through less certainty as well as the customer through higher prices. Thus, customers could be deprived of a contractual instrument to negotiate ex-ante benefits and cloud service providers may be more constrained in their ability to pass on efficiencies to customers. This could hurt especially customers who face other costs of switching and thus expect to remain in a longer-term relationship with a particular cloud service provider anyway.

Regulation of discounts and cloud credits: Key trade-offs and considerations

Interventions into the pricing practices of cloud providers with respect to committed spend discounts and cloud credits involve risks of inadvertently constraining competition and thus lowering the direct (often short-term) benefits available to customers. This is particularly the case if other significant switching costs for customers persist. Moreover, there are particular innovation and efficiency benefits from committed spend discounts and cloud credits being available as pricing instruments to cloud providers (such as greater investment certainty for service providers and reduced market entry costs for customers). Hence, any potential benefits from intervening in these pricing practices in terms of lower switching costs or remedying any anti-competitive effects should be carefully weighed against these risks and negative side effects for customers.

[239] See also Farrell & Klemperer, 2007 (n 115).

Non-discrimination obligations may benefit existing customers at the expense of new customers, but the overall net benefit for customers is unclear and rather likely to soften overall competition.

5.5 Interoperability Regulation

Data portability and application portability address switching costs from the incompatibility of substitute services between cloud providers. However, there may also arise switching costs from the incompatibility of complementary services (see Section 4.1). In particular, this is the case if a customer wants to migrate one of its services to another service cloud provider but retain other services of the same service ensemble at the original service provider. In this case, interoperability, that is, the ability of services to exchange compatible messages during runtime, facilitates multi-cloud approaches that allow for the interconnection of services across providers (see Section 2.1). This can reduce the switching costs for services if they operate as part of a customer's service ensemble. Furthermore, interoperability and multi-cloud approaches can facilitate market entry and growth of more specialised cloud operators, as customers can more easily 'mix and match' services of different providers, instead of relying on provisioning all services from the same cloud service provider. However, even with increased interoperability, operational challenges inherent to multi-cloud approaches are likely to persist (see Section 4.1)

In general, interoperability of cloud services is a very broad concept that can pertain to many different use cases and requirements.[240] In the following, we focus on approaches aimed at facilitating interoperability for multi-cloud solutions and the interconnection of cloud services across providers, as described above. In this context, it is important to note that interoperability, although often referred to as a global concept for cloud computing, must technically be established with reference to specific cloud services and their respective functions and requirements.[241] Moreover, as discussed in Section 2.1, there are different means to achieve interoperability of cloud services: by standardisation or by syntactic and semantic interoperability between services.[242] Both approaches usually rely on the exposure of APIs and their accessibility by other services as well as a shared understanding between the services of the API's specification and functions. Hence, whereas a common standard for a service or interface specification is technically the most straightforward way to establish interoperability, there also exist alternative approaches based on technical converters and abstraction layers that serve as 'bridges' or 'gateways' between otherwise non-interoperable services, which may, however, add technical complexity and implementation overhead (see Section 4.1).

5.5.1 Mandatory standardisation through regulation

The lack of common standards in many areas of cloud computing is not because of a lack of technical proposals for interoperable standards. In fact, it has been noted that "[t]here are many cloud

[240] Godlovitch, I. & Kroon, P. (2022). Interoperability, switchability and portability – Implications for the Cloud. https://www.wik.org/fileadmin/files/_migrated/news_files/WIK-C_Studie_Implikationen-fuer-die-Cloud.pdf
[241] Cf. Lewis, 2013 (n 230).
[242] Kaur et al., 2017 (n 18).

standardization projects — maybe too many".[243] Instead, the main challenge has proven to be establishing common standards that can satisfactorily capture the differentiated specialisations, the wide variety of features, and the heterogeneous technical implementations of cloud services. This is further complicated by the continuous evolution of existing services and the introduction of new services. In addition, cloud service providers' interests, especially of providers that offer integrated services ecosystems, will often favour proprietary solutions over common and open standards, which can inhibit standardisation procedures as well as the adoption of common and open standards.

Mandatory standardisation through regulation (see, for instance, the interoperability provisions in the DA) can remedy the latter obstacle to some extent by forcing cloud providers to comply with specified standards for specific services and their interfaces. However, such mandatory standards face the same challenges as previous standardisation initiatives and run the risk of hurting cloud providers and customers by locking the industry into specific standards. This is especially the case if a mandatory standard must be supported by any service of a cloud service provider that falls in the same 'service type' as specified by the standard. In this case, the negative effects of limiting the diversity and variety of service implementations and constraining innovations through mandatory, pre-specified standards are the highest.[244] Moreover, the procedures for establishing such mandatory standards present significant challenges themselves, which could especially complicate the evolution and updating of such standards over time.[245]

These challenges and costs must be weighed against the benefits of a specific mandatory standard in terms of customers' improved ability to switch between cloud providers and the additional innovation opportunities offered to cloud providers. In this vein, a mandatory standard should only be considered in cases where:

(i) the lack of interoperability presents a significant barrier for customers to interconnect services across providers in order to establish multi-cloud solutions;

(ii) there are significant benefits for customers from interconnecting the service(s) in question across providers (considering also the remaining operational challenges involved with such interconnection); and

(iii) a standard is expected to significantly facilitate the provision of complementary services.

Even then, the identified benefits should be weighed against the case-specific costs that derive from the negative effects of mandatory standardisation in the specific application context, especially on innovation and differentiation as discussed above. Importantly, several benefits of standardisation may only develop over time after a standard is established. Nonetheless, there should be reasonable expectations of these benefits with reference to the specific service in question when imposing a mandatory standard.

The negative effects of mandatory standardisation may be mitigated by requiring cloud providers to offer at least one service that complies with an obligatory standard, but allow providers to also offer

[243] Lewis, 2013, p. 1653 (n 230); Fogarty, K. (2011). Cloud Computing Standards: Too Many, Doing Too Little. https://www.cio.com/article/282352/cloud-computing-cloud-computing-standards-too-many-doing-too-little.html
[244] Cf. Ennis & Evans, 2023 (n 16).
[245] Cf. Schnurr, 2023 (n 17).

additional services of the same service type that do not necessarily comply with the standard. Such a regulatory approach would aim to ensure that customers can choose between the benefits of interoperable services and the benefits of non-standardised, more differentiated services. Such an approach is not chosen in the DA but could be considered as an alternative approach to mandatory standards (see Section 3.2.7). While such an approach would strive to combine the need for interoperability with more freedom for innovation, it is likely to be less effective in achieving effective interoperability, as cloud providers could have an incentive to steer customers towards non-standardised services (for instance, by offering a lower price for such services) and prioritise the development of proprietary services. Whereas additional non-discrimination obligations and regulations could provide safeguards in this regard, enforcement would require more extensive regulatory intervention.

5.5.2 Open APIs and transparent interface specifications

As an alternative to mandatory standards, regulation may aim to promote interoperability by ensuring that APIs of certain services are discoverable, accessible, and transparent about their specifications. This does not directly ensure interoperability but can facilitate the development of targeted convertors or software tools by destination cloud providers, by third parties, or by customers themselves that then allow customers to interconnect services and establish multi-cloud solutions (see also Section 4.1). By avoiding obligatory standards for specific services, such an approach would leave more flexibility to cloud providers and more freedom for innovation and the development of differentiated services. Therefore, this approach could mitigate several of the above-mentioned negative effects of mandatory standardisation.

At the same time, such flexibility and freedom could represent a critical and particular shortcoming from the perspective of customers, third parties, and cloud service providers that would rely on such APIs to establish interoperability through custom-made software and additional abstraction layers. Many cloud services are based on numerous APIs and protocols that can be difficult to manage as public-facing APIs. This is especially the case because public APIs are designed for resilience, security, and stability, whereas internal APIs are often designed to be flexible and are frequently changed to accommodate new features and operational requirements. As market-driven and custom-made interoperability solutions critically depend on cloud providers' exposed service APIs and a shared understanding of the semantics of the services' functions and data, any decision of a cloud provider to change, modify, or even abandon APIs or underlying service functions represents a significant risk to the technical operations of such interoperability solutions. In consequence, these uncertainties and risks can discourage customers from adopting multi-cloud approaches resting on such custom-made interoperability solutions.

To promote these market-driven and custom-made interoperability solutions, regulation could therefore stipulate additional safeguards on the availability and longevity of exposed service APIs. In this vein, obligations may not only impose requirements on the availability of APIs and their documentation but may additionally stipulate that any changes to the API need to be announced with a pre-specified lead time to give providers of custom-made interoperability solutions sufficient time to implement the necessary changes in their own software. Similarly, it may be required that the APIs in question cannot be suddenly and unexpectedly terminated (unless justified by exceptional

circumstances such as significant security risks) but must allow for a sufficient expiration period that can allow custom-made interoperability solutions to implement alternative interfaces. Of course, such safeguards and additional obligations on the cloud service provider, depending on the precise requirements, can entail several negative effects that are qualitatively similar to those of mandatory standards, including reducing the flexibility of cloud service providers and thus possibly the pace of innovation. In the case that cloud service providers would need to expose services' internal APIs there could arise an additional risk that competitors may be able to reverse-engineer the underlying structure or logic of proprietary services. However, by giving cloud service providers considerably more flexibility and freedom with respect to the commercial design and technical implementation of their services than under mandatory standardisation, such a regulatory approach could be leveraged to balance the benefits and risks associated with promoting interoperability for multi-cloud solutions.

Interoperability regulation: Key trade-offs and considerations

Promoting interoperability through regulation can have pro-competitive effects by facilitating multi-cloud approaches for customers and facilitating specialised service offers by providers that do not offer a broad range of cloud services. The benefits and costs of interoperability regulation must be assessed with reference to specific cloud services and use cases, and should also consider the general operational challenges inherent to multi-cloud approaches that are not related to interoperability.

Mandatory standards are the most effective and straightforward way to establish interoperability but can entail significant negative effects on cloud providers' flexibility and freedom to differentiate their services. This can reduce service variety and impede innovation. These negative effects may be reduced by allowing cloud providers to offer proprietary service implementations in addition to standardised services. In light of the significant risks and costs of mandatory standards, there should be strong evidence for the case-specific benefits of such intervention.

Regulation may also aim to promote market-driven and custom-made interoperability solutions that can bridge heterogeneities between providers' services. To this end, regulation may require cloud service providers to make APIs and accompanying documentation for specific services available. In addition, regulation may impose safeguards against sudden changes and termination of these interfaces. These restrictions on cloud providers' freedom have similar but likely less significant negative effects than mandatory standards, as they preserve more flexibility and freedom for cloud providers and their service offerings.

6. CONCLUSIONS AND RECOMMENDATIONS

The rapid and ongoing growth of the cloud computing industry highlights the central role of cloud infrastructures and services for the current and future European digital economy. As a key input and enabler of digital services, cloud computing has a large-scale impact on competition and innovation in a wide range of digital markets. By establishing a common computing and data infrastructure, cloud computing further raises overarching questions on the protection of cyber security and privacy as well as with respect to broader policy goals, such as national security or industrial policy goals.

As a consequence of the technical progress, the economic importance and the general societal relevance of cloud computing, there has been a myriad of cloud policy initiatives at the EU level during the current Commission under President von der Leyen. Several of these policy initiatives have recently been adopted as regulations, most notably the Data Act and Digital Markets Act, while other initiatives and issues continue to be debated. At the same time, there are ongoing investigations on the national level into the cloud computing industry with a focus on competition issues and the proper functioning of these markets. Finally, there are also several European-wide stakeholder initiatives, for example, with the aim to facilitate interoperability among European cloud computing providers.

Given these numerous developments and major policy updates, this CERRE research report takes stock of the recent developments and major policy updates in the EU with a focus on competition and the proper functioning of markets in the cloud computing industry. In particular, the report aims to provide a broad review of recent policy initiatives but focuses in its analysis on competition issues in cloud computing, which are considered to be central to the broader EU cloud computing policy framework. As such, policy initiatives aimed at enhancing cybersecurity are considered only for their potential impact on competition. Furthermore, the legal assessment aims to provide a cross-cutting analysis of all pieces of legislation involved in cloud regulation by selecting the relevant provisions for the policies that have a broader scope as well as by attempting systemic interpretations of provisions enshrined in different acts, yet, directly or indirectly, interplaying.

To this end, the report provides a coordinated legal review and analysis of the recent policy initiatives as well as an economic analysis of the competition issues that arise with regard to the specific economic and technical characteristics of the cloud computing industry. In this vein, the report analyses potential reasons for market inefficiencies in the cloud sector that can justify policy interventions from an economic perspective and highlights the economic trade-offs that arise in the context of different regulatory approaches and remedies. Consistently, the report describes some inaccuracies and contradictions in the existing regulation, deriving from economic and technical peculiarities of the cloud services (vis à vis other digital services and markets) that may have been neglected or underestimated.

In this vein, the report provides an economic and legal assessment of the recently adopted policies and regulations as well as their justifications from an economic perspective. Furthermore, the report contributes to the ongoing and future policy process by providing an analysis that can inform the interpretation and implementation of already adopted regulatory policies such as the Data Act as well as decisions on future cloud policies and interventions at the EU and national level. From a legal

perspective, the report highlights several areas where further clarification is required with respect to the adopted and proposed policies and their precise interpretation. Moreover, the analysis identifies several problems of coherence and consistency between different regulations. From an economic perspective, the report provides a framework to assess the economic justifications and implications as well as the trade-offs that arise for the implementation of specific regulatory approaches and remedies in cloud computing.

Overall, it is important to consider the specific economic and technical characteristics as well as the current state of the European cloud industry as briefly summarised at the beginning of this report (see Section 2). In particular, it is vital to recognise the different cloud service models, the variety of services, use cases and customer needs, and the core technical principles that cloud computing services are built on (see Section 2.1.2). From a regulatory perspective, central concepts such as interoperability and portability must be clearly delineated with respect to their technical requirements and their potential benefits for competition and innovation in order to integrate these technical concepts into effective policies (see Section 2.1.1).

Based on the legal and economic analysis in this report, we derive the following six overarching recommendations:

Recommendation 1: The legal interpretation within and across policies should be clarified by providing guidelines in order to address problems of coherence and cross-consistency as well as to reduce uncertain legal interaction effects, also by issuing the Cloud Rulebook.

EU legislation and policies about cloud services comprise several different pieces of legislation and actions, covering technological, economic, and legal aspects, and aiming at different kinds of results in terms of competition, competitiveness, and consumer protection (see Section 3). Coherence and cross-consistency of all regulations, ranging from a clear and consolidated definition of the main legal concepts involved to their respective scopes of application and their possible interplays, should be a primary objective both when conceiving the substantial rules and when drafting the legal documents. With respect to the current EU policy framework, this has been found particularly important for obligations concerning data portability, (vertical and/or horizontal) interoperability, and functional equivalence, primarily in the DA (see Section 3.2) yet also across other pieces of legislation when these concepts are adopted. To a certain extent, this problem could and should be tackled through the long-awaited Cloud Rulebook, which may play a crucial role in providing extensive clarifications, albeit non-legally binding, based on a systemic interpretation of all pieces of legislation involved in cloud regulation, as well as providing clarifications on whether and where the adopted voluntary self-regulatory codes are still playing a role in the cloud regulation.

Recommendation 2: As for the DMA enforcement, the Commission should thoroughly consider all specific features of cloud services vis à vis other core platform services, in particular, by applying the proportionality principle, both to the designation of gatekeepers and to the application of remedies, in order to avoid internal incoherence and regulatory anomalies.

The DMA is of pivotal importance for competition policy and consumer/business users' empowerment in digital markets. However, because of the many nuances and specificities of cloud services as core

platform services, that is, primarily the overall lack of two-sidedness (except for marketplaces, see Section 4.2.2), it is extremely difficult to find a systemic interpretation of the basic concepts of end users, business users, and gatekeepers under the DMA (see Sections 3.3.2 and 3.3.3). In turn, this can make it very difficult to have a designation of cloud service gatekeepers that is at the same time both operational and meaningful under an economic regulation perspective. Moreover, only a subset of DMA obligations seems to be relevant and applicable in the context of cloud computing (see Section 3.3.4). To soften these pitfalls and to mitigate the risks of unintended consequences, the DMA should be interpreted and applied considering the proportionality principle, which is explicitly mentioned in the DMA at Recital 28 for emerging undertakings. According to the proportionality principle, each regulatory measure should be meaningful and necessary to reach the regulatory objective when the same result can't be achieved by putting in place a less intrusive action. Operationally, this should translate into considering all the basic concepts for gatekeepers' designation as well as for possible rebuttal actions in a coordinated and consistent fashion, and, in case of designation, in imposing only a subset of obligations that are meaningful considering the market structure of a gatekeeper for cloud services.

Recommendation 3: Establish a clear institutional framework for the enforcement of the existing rules to avoid too much fragmentation.

The DMA and the DA are two distinct pieces of regulation, and this report has identified potential inconsistencies between the two, which may (or may not) produce enforcement problems. There is a risk that their parallel application could create uncertainty, and this risk is magnified by the differences in enforcement setting (see Section 3.4.2). Indeed, the strikingly asymmetric institutional design of the DA vis à vis the DMA could result in a problematic lack of coordination in the application of the two pieces of legislation. Moreover, fragmentation within the national enforcement level should be avoided. These problems could be addressed, inter alia, by: (i) maintaining a decentralised enforcement for the DA, yet establishing strong formal coordination mechanisms (as it is the case for telecom NRAs, BEREC and EU Commission for example); and (ii) reducing national fragmentation by allocating new competences defined by the DA to already existing national authorities (as defined in previous EU legislation). This would not go against the principle that each Member State is competent to identify and designate national enforcers, as the EU rules would only identify bundles of competences (defined in different normative acts), in an abstract manner, which will be detailed by each member state; and (iii) the European Commission should exercise its discretion toward a clearer centralisation for EU competition law enforcement in digital markets and services regulated by the DMA, especially when gatekeepers are under investigation, in order to avoid legal uncertainties.

Recommendation 4: Regulatory interventions should consider the specific economic and technical characteristics of the cloud computing industry as well as the strategic decision-making of cloud customers. In general, there is evidence of competition among cloud providers, especially for customers who migrate to the cloud for the first time. However, competition concerns may arise from factors that facilitate vendor lock-in, particularly when markets are concentrated because of significant economies of scale and scope.

The review of European policy initiatives demonstrates that several of the recent policy interventions have been motivated, among other factors, by concerns about the proper functioning of markets in the cloud computing industry. In particular, the recently adopted DA aims to facilitate customer switching and multi-vendor cloud approaches by introducing a range of new cloud regulations (see Section 3.2). Among others, these regulations aim at facilitating data portability, lowering contractual barriers to switching, reducing and even fully eliminating data egress fees as financial switching costs, achieving functional equivalence at the IaaS service layer, as well as promoting interoperability through the possibility of mandatory standards and service specifications.

In our analysis of competition issues, we focus on whether vendor lock-in and economies of scale and scope give rise to market inefficiencies (that is, market outcomes that deviate from the first-best outcome that would maximise social welfare) that could justify regulatory intervention from an economic perspective (see Section 4). In this vein, our analysis of the underlying economics of cloud computing can inform the assessment and implementation of the recently adopted provisions of the DA but also serve as a guiding framework for future cloud policy initiatives. Importantly, our analysis highlights that cloud computing services share some key economic characteristics with other digital services (such as the competition between integrated providers of service ecosystems and specialised complementors) but differ in other important aspects (such as the pipeline value chain structure of cloud computing as opposed to two-sided markets of digital platforms).

Economies of scale and scope represent key characteristics of cloud computing services. In particular, at the IaaS layer, economies of scale can facilitate concentration when not offset by the benefits of specialisation. In consequence, one can expect that the mainstream of IaaS services will be provided by a smaller number of large providers as the industry matures. Nonetheless, there are indications of competition between providers of IaaS services in today's markets, even though a large share of the markets, including the take-up of new customers, is captured by large cloud service providers, known as hyperscalers. Compared to the IaaS layer, market entry at the PaaS layer and the SaaS layer is significantly easier, as application developers and service providers can make use of cloud infrastructure services themselves. In turn, this can raise concerns about a competitive level playing field when independent software vendors (ISVs) compete with the same hyperscalers that they also rely on with respect to access to IaaS services (see Section 4.2.2). Even if ISVs do not rely on competitors' IaaS services, integrated cloud providers frequently have a competitive advantage due to their ability to offer ecosystems with a broad range of services. However, these integrated ecosystems also offer benefits and efficiencies to customers due to economies of scope and benefits from the technical integration of cloud services.

Overall, the cost and demand characteristics of cloud services give rise to a general welfare trade-off between efficiencies from large-scale operations and integrated ecosystems, on the one hand, and higher concentration among cloud service providers, on the other (see Section 4.2.3). Therefore, we suggest that the general focus of regulation and competition policy should be on (i) monitoring the ability of ISVs to enter and compete with respect to their specific services markets, and (ii) safeguarding and promoting competition intensity by reducing switching costs to the extent this promotes the lock-in of customers.

Although customers face switching costs in many markets, cloud computing services exhibit several specific types of switching costs, which can arise from technical and financial barriers to switching. Consequently, the possibility and extent of vendor lock-in in cloud computing are determined by the interplay of different types of switching costs and the sum of switching costs that accumulates for customers. When assessing the competitive implications of switching costs, it is important to consider customers as strategic actors and the extent of their ability in specific markets to negotiate ex-ante benefits that can compensate for higher long-term prices due to the presence of switching costs.

In general, we consider that data-induced switching costs, technical incompatibility and data egress fees can together constitute significant costs for switching and may give rise to vendor lock-in for certain types of customers and services. These switching costs can result from both the strategies and actions of the cloud service provider as well as the customers' demands and decisions (see Section 4.1.1 to 4.1.3). Whereas committed spend discounts can add to the switching costs of customers, these and similar practices (like cloud credits) are associated with direct (often short-term) benefits for customers and any regulatory intervention should therefore be treated with particular caution. With respect to interoperability, our analysis highlights that, in the context of vendor lock-in, interoperability may not be seen so much as an ultimate and universal end in itself, but as a potential means to decrease switching costs from technical incompatibility. In particular, by facilitating multi-cloud approaches, interoperability could provide customers with a more credible threat of switching, thus improving their negotiation position vis-à-vis their current cloud provider (see Section 4.1.2). Overall, our analysis highlights that the identified types of switching costs can often result from a range of different motives of cloud service providers and therefore regulatory interventions are likely to have manifold economic effects.

Recommendation 5: Remedies to address competition concerns in cloud computing involve important and manifold economic trade-offs. In general, our analysis suggests that remedies, which directly limit the (often short-term) benefits of customers (such as interventions into committed spend discounts and cloud credits), should be treated with particular caution, whereas data portability regulation and cost-based regulation of data egress fees are better suited to address structural barriers to switching and multi-cloud approaches.

Based on our analysis of the economic trade-offs that arise from different regulatory approaches and remedies (see Section 5), we suggest that regulatory intervention should prioritise addressing structural barriers to switching and multi-cloud approaches. To minimise adverse effects from regulatory intervention, we argue that remedies should focus on empowering customers as strategic actors that internalise the central trade-off between short-term benefits and long-term costs of cloud service adoption and multi-cloud cloud approaches.

In this vein, we view data portability as a promising general approach to address technical barriers to switching providers (see Section 5.1). Although data portability incurs implementation costs for cloud service providers and regulatory costs for oversight and enforcement, these costs as well as the associated technical complexity are generally lower than for application portability approaches. To limit implementation costs and complexity, we suggest that the default requirement for portable data should be to make data available to customers in a structured, commonly used, open and machine-

readable format. Hence, we believe that the criteria imposed by Article 30 (5) of the Data Act represent a suitable default for data portability. In contrast, mandatory standardisation of data formats (as under Articles 30 (3) and 33 DA) should be limited to selected cases, where services are more clearly homogeneous to a certain degree, markets are concentrated, and data portability is of high value to customers. Furthermore, we consider one-off data portability to be sufficient for many cases of customers switching providers, whereas continuous data portability facilitates interconnection and thus multi-cloud approaches. These considerations may serve as guidelines for the implementation of data portability obligations under the Data Act.

Compared to data portability, application portability can further reduce technical barriers to switching for customers (see Section 5.2). However, application portability is significantly more challenging to achieve from a technical perspective, as it requires interoperability of the portable service with underlying cloud services and native functions of a cloud provider's environment. The technical complexity for achieving application portability generally increases with higher layers of the cloud stack due to more complex dependencies. Although mandatory standardisation is most effective in achieving seamless data portability, there are, in general, significant welfare costs in terms of constraining innovation and service differentiation. Furthermore, mandatory standards may also hurt customers by limiting availability and benefits from proprietary, integrated service offerings. Hence, early policy interventions, such as those relating to the implementation of Article 33 of the Data Act, may instead focus on promoting voluntary interoperability frameworks that increase the transparency of service dependencies across providers.

Price regulation of data egress fees can decrease financial switching costs and thus reduce the risk of vendor lock-in. Regulatory intervention directly lowers the costs of switching for customers that need to transfer large data volumes as well as more indirectly lowers the costs for switching that arise from barriers to multi-cloud approaches. This comes at the cost of limiting cloud providers' freedom to set prices and entails the risk of distorting price signals. Whereas price regulation can have pro-competitive effects by reducing potentially excessive prices, there is the risk that service providers will recoup the costs of external data transfers through increased prices for all cloud users (see Section 5.3). In line with the DA's provisions on data egress fees for the general operations of multi-cloud approaches (Art. 34 (2) DA), we consider cost-based price regulation a suitable approach to balancing this trade-off if financial switching costs are found to constitute a significant barrier for switching or for establishing multi-cloud approaches. We suggest that transit prices may serve as a market-driven benchmark and general proxy for cost-based regulation of egress fees. In contrast to the DA's provision on data egress fees for the purpose of switching (Art. 29 (1) DA), we generally advise against a zero-price regime for data egress fees. Whereas such an approach fully eliminates data-related financial switching costs for customers and therefore could benefit smaller providers through increased customer switching, it prohibits cloud service providers from directly recovering any of the costs for external data transfer, which creates socially inefficient incentives for providers and customers. Furthermore, if applied symmetrically as by the DA, a zero-price regulation could pose a substantial business risk for smaller providers, as cross-subsidisation of data traffic costs is more difficult for those providers.

Finally, we highlight that interventions into the pricing practices of cloud providers with respect to limiting or prohibiting committed spend discounts and cloud credits involve risks of inadvertently constraining competition and thus lowering the (often short-term) benefits of competition made available to customers (see Section 5.4). This is particularly the case if other significant switching costs for customers persist. Hence, any (mostly long-term) benefits from intervening in such pricing practices in terms of lower switching costs or remedying anti-competitive effects should be carefully weighed against the general risks of limiting competition and hurting customers. In addition, there are particular innovation and efficiency benefits from committed spend discounts and cloud credits being available as pricing instruments for cloud providers. Non-discrimination obligations on these pricing practices may benefit existing customers at the expense of new customers, but the overall net benefit for customers is unclear and could likely be detrimental to overall competition.

Recommendation 6: Regulatory efforts to promote interoperability for multi-cloud approaches should aim to facilitate and safeguard the development of market-driven interoperability solutions that can bridge heterogeneities between providers' services. Mandatory regulated standards should be considered as a last resort, as expected benefits must be significant to exceed the general negative effects and challenges of enforced standardisation.

Data portability and application portability address switching costs from the incompatibility of substitute services between cloud providers. However, there may also arise switching costs from the incompatibility of complementary services (see Section 4.1.3). In particular, this is the case if a customer wants to switch one of its services to another service cloud provider but retain other services of the same service ensemble at the original service provider. In this case, interoperability, that is, the ability of services to exchange compatible messages during runtime, facilitates multi-cloud approaches that allow for the interconnection of services across providers. This can reduce the switching costs for services if they operate as part of a customer's service ensemble (see also Section 4.1.3). Furthermore, interoperability and multi-cloud approaches can facilitate market entry and growth of more specialised cloud operators, as customers can more easily 'mix and match' services of different providers, instead of relying on provisioning all services from the ecosystem of the same cloud service provider. However, there are operational challenges inherent to transferring data between locations and providers that are likely to persist even with interoperability.

Technically, interoperability between services can be achieved either by standardisation or by syntactic and semantic interoperability between services (see Section 5.5). Syntactic interoperability refers to the ability to exchange data and semantic interoperability refers to the ability to operate on that data according to agreed-upon semantics. Syntactic interoperability is enabled by the exposure of an API and its accessibility by other services, whereas semantic interoperability requires a shared understanding between the services of the API's specification and functions. Although often referred to as a global concept for cloud computing, the benefits and costs of interoperability regulation must be assessed with reference to specific cloud services and use cases.

Mandatory standards (as envisioned by Art. 33 DA) are the most effective way to establish interoperability but entail significant negative effects on cloud providers' flexibility and freedom to differentiate their services (see Section 5.5.1). This can reduce service variety and impede innovation.

Moreover, the procedures for establishing such mandatory standards present significant challenges themselves, which could especially complicate the evolution and updating of such standards over time. The negative effects of mandatory standards may be mitigated to some degree by allowing cloud providers to offer proprietary service implementations in addition to standardised services. However, in light of the significant risks and costs of mandatory standards, there should be strong evidence for the case-specific benefits of such intervention. Therefore, we recommend that the interoperability provisions should only be used in cases, where there is clear evidence of market failures and other measures fail to promote competition.

As an alternative, regulation may aim to promote market-driven and custom-made interoperability solutions that can bridge heterogeneities between providers' services (see Section 5.5.2). To this end, regulation may require cloud service providers to make APIs and accompanying documentation available for specific services. In addition, regulation may impose safeguards against abrupt changes and termination of interfaces with the exception of explicit and specific threats to the security or integrity of cloud services. These restrictions on cloud providers' freedom have similar but likely less significant negative effects than mandatory standards, as they preserve more flexibility and freedom for cloud providers and their service offerings.

cerre Centre on Regulation in Europe

Avenue Louise 475 (box 10)
1050 Brussels, Belgium
+32 2 230 83 60
info@cerre.eu
www.cerre.eu

Centre on Regulation in Europe (CERRE)
CERRE Think Tank