WIK-Consult • Report

Study for Microsoft

Interoperability, switchability and portability – Implications for the Cloud

Authors:
Ilsa Godlovitch
Peter Kroon

Bad Honnef, 4 November 2022

WIK CONSULT

Imprint

WIK-Consult GmbH
Rhöndorfer Str. 68
53604 Bad Honnef
Germany
Phone: +49 2224 9225-0
Fax: +49 2224 9225-63
eMail: info@wik-consult.com
www.wik-consult.com

Person authorised to sign on behalf of the organisation

General Manager	Dr Cara Schwarz-Schilling
Director	Alex Kalevi Dieke
Director Head of Department Networks and Costs	Dr Thomas Plückebaum
Director Head of Department Regulation and Competition	Dr Bernd Sörries
Head of Administration	Karl-Hubert Strüver
Chairperson of the Supervisory Board	Dr Thomas Solbach
Registered at	Amtsgericht Siegburg, HRB 7043
Tax No.	222/5751/0926
VAT-ID	DE 329 763 261

Contents

1 Executive Summary

1.1 Background

Cloud computing is an important enabler for the digital economy. In addition to reducing costs, cloud computing can improve access to advanced IT solutions, boosting innovation[1] and productivity across a wide range of sectors,[2] which is vital in supporting sustainable growth and recovery following the challenges of COVID and the energy crisis. In its vision for Europe's Digital Decade,[3] the European Commission has established a target that 75% of EU companies should make use of technologies such as cloud computing, AI and big data. This will require significant efforts to boost take-up as in 2021, only 41% of companies in the EU were using cloud computing and a significant proportion of cloud usage is limited to basic services like mail and file storage.

As cloud computing has gained momentum, there has been an increasing focus on the need to ensure that customers can make use of multiple services and are not locked into their cloud provider(s), and that providers of cloud computing services that are found to be "gatekeepers" do not exploit this position to undermine fairness and contestability. These concerns underlie the adoption of certain provisions in the Digital Markets Act,[4] as well as proposals in the draft Data Act,[5] concerning cloud interoperability and portability.

This study seeks to provide insights on the meaning of cloud services, how interoperability and portability have been applied in the other sectors such as telecoms and banking and the circumstances in which these concepts may be relevant to the cloud. We consider the implications of this analysis for the ongoing review of the Data Act.

1.2 What is meant by the cloud?

Cloud computing is the delivery of computing services—including servers, storage, databases, networking, software, analytics, and intelligence—over the Internet. It offers an alternative for customers deploying their own, on-premises IT infrastructure and applications, and in doing so saves cost (and in particular capex) as well as offering

1 Carlos Moedas, Commissioner for Research, Science and Innovation, noted in May 2018 that „The Cloud will be a game changer for science in Europe." European Commission, Directorate-General for Research and Innovation, Horizon Europe: strategic plan 2021-2024, Publications Office, 2021, https://data.europa.eu/doi/10.2777/083753

2 Various studies have highlighted the potential for cloud computing to boost productivity across the wider economy. See for example LSE (2019), https://www.lse.ac.uk/business/consulting/reports/the-transformative-effect-of-cloud-on-firm-productivity-and-performance#:~:text=This%20research%20indicates%20that%20cloud,%2C%20location%2C%20size%20or%20sector

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

4 https://www.europarl.europa.eu/doceo/document/TA-9-2022-0270_EN.html

5 https://digital-strategy.ec.europa.eu/en/library/data-act-proposal-regulation-harmonised-rules-fair-access-and-use-data

access to state-of-the-art hardware and applications that customers would otherwise not be able to replicate.

Cloud services have traditionally been categorised into Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS), although the distinctions are fluid.

Whereas a private cloud is deployed for only one customer, public cloud serves multiple customers, bringing benefits in flexibility and cost. Customers can use multiple public clouds to access the same or different applications. These are called multi-cloud solutions.

The cloud market is very diverse, with multiple specialised niches and many different suppliers. On a wide interpretation, enterprise customers that develop and offer services in the cloud could also be said to be cloud providers.

1.3 What is meant by interoperability, portability and switchability?

Interoperability refers to the degree to which two or more systems, products or components can exchange information and make use of the information exchanged. It is possible to identify different degrees of interoperability, from no interoperability to full interoperability. Horizontal interoperability refers to communication between two systems at the same level of the value chain, while vertical interoperability refers to interaction at different levels of the value chain e.g. to develop applications on a platform, or add-ons to software. Portability refers to the potential to export or transfer data, applications or platforms from one IT system to another. This potential might vary but will often not be 100% because applications and underlying IT systems will always have certain differences.

In the context of cloud, interoperability can be defined with reference to the ISO “5 facet” model, which distinguishes different levels of interoperability from transport of data through to mutual recognition of data formats, interpretation of the data and finally the ability of two systems to deliver expected results. Compatibility of legal norms including the treatment of data is also relevant when considering the degree to which two systems can be fully interoperable. Cloud portability can involve porting (virtual) “infrastructure” from on-premises data centres to the cloud or between different clouds, through to the porting of platforms, applications and data.

There is no generally accepted definition for "switchability”, but it could refer to the ease with which end-users can switch from one service or system to another. It could involve, alongside the porting of any required data or applications, the ease of terminating the contract with one party and subscribing with another (and associated timeframe and cost). However, it should be noted that switching implies that one service is being terminated in order to move to an alternative supplier, which the customer views as a substitute. As such, it is more meaningful in relation to services which are characterised by “single homing” and involve limited differentiation, which is often not the case for cloud services.

1.4 How have interoperability and portability been applied in other sectors?

Interoperability and portability obligations have been successfully introduced, most notably in telecoms and banking. However, in these cases, interoperability has been service-specific and focused on basic functions such as calls and details which are essential for inter-bank communications while portability has focused on specific key data points. Even with this limited scope, experience shows that introducing standards and consequent implementation of interoperability involved considerable time (multiple years) and effort on the part of the industry. Other basic online services such as email (and USENET) were designed to be interoperable from the outset.

Where *horizontal* interoperability has been implemented on the basis of common standards (such as in voice, SMS, email interconnection), there has been limited subsequent innovation in the service concerned. Rather, innovation has flourished in the surrounding unregulated environment, as can be seen for example in the case of OTT NIICS services such as video conferencing and messaging applications.[6]

Data portability (including deadlines) has played a crucial role in facilitating switching both in the telecoms and banking sectors. However, there are important differences between these services and the cloud. Firstly, in contrast with cloud, where services are diverse, telecoms and banking and the associated data points (such as the telephone or bank account number, standard transactions), are clear, commonly applied and understood, and portability obligations have focused on these relatively simple, basic and limited datasets. Secondly, telecoms and banking are essential “universal” services for which customers typically have one main provider (and thus switching with the portability of the identifier is a key element in supporting competition), in contrast with cloud services where services are not “universal” and multi-homing is more common.

---

6 In contrast, the “open banking” provisions show that *vertical* interoperability can support “over-the-top” innovation. However, to be effective, it is necessary for the measures to be focused on specific applications and/or data points where there is scope for additional innovation benefiting customers and application providers are ready to engage.

1.5 Where could interoperability and portability potentially apply in the cloud?

Porting and interoperability can be relevant at various stages in the customer journey for cloud including: (a) migrating from an on-premises solution to the cloud or adding additional cloud native applications; (b) linking the remaining on-premise servers or applications with the cloud (hybrid cloud); (c) making use of services from different cloud providers (multi-cloud); (d) building on cloud platforms or applications to add further functionality; and (e) switching from one cloud service provider to another.

The process of IT migration in general for an enterprise is project-based and can take several months or more depending on the scale of the enterprise and the number of integrations with other products and entities. The complexity, time and cost are likely to depend on customer choices about which services to procure from the cloud, the complexity of applications and the size of databases and data that they plan to move. Tools provided by cloud service providers may help to streamline the process in some cases, but it is inevitable due to the diversity of the choices for the customer and products involved that this process will be project-based.

Enterprise customers are increasingly linking their on-premises and cloud capabilities and making use of multi-cloud solutions. This may require a degree of interoperability. This is well-established at the IaaS layer e.g. where two cloud services have a common understanding of data models such as virtual machines and containers, but becomes increasingly complex further up the value chain as different providers distinguish their platform capabilities and services are diverse. Nonetheless, standards have been developed to support data exchange and aid recognition of common formats, and some service providers encourage “over-the-top” innovation by publishing APIs.

Data portability and switching may also be relevant for consumers, who make use of “SaaS” services such as content lockers, cloud-based productivity software or back-up. In addition to consumers’ right to download their personal data, consumer SaaS switching can be facilitated by using standardised file formats e.g. for video-encoding or through conversion tools. However, equivalence of functionality cannot be achieved without undermining the potential for different applications to differentiate their services, innovate, and compete.

1.6 Implications for the draft Data Act

The draft Data Act proposes a raft of obligations on cloud service providers which include an obligation for the donor CSP to allow contract termination within 30 days, and to “ensure”, full continuity in the provision of functions and services. The Data Act also includes far-reaching obligations for interoperability standards, including a goal of achieving functional equivalence between services from different providers. These proposed obligations are likely to be challenging to interpret, implement and enforce, and could undermine choice and innovation. Specifically:

- Cloud computing includes a vast range of different kinds of services. Horizontal interoperability and switching is not meaningful in a generic sense, but only in relation to specific cloud services or data. Thus, a generic goal to achieve interoperability or support switching is unlikely to provide clarity to the market or deliver concrete results.
- A requirement or goal to achieve “full equivalence“ by interoperability and service continuity“ in switching leaves little room for differentiation between services and would consequently serve to limit choice and innovation to the detriment of customers.
- The proposal that cloud service providers should provide 30 day contract termination and support switching free of charge is unsuited to enterprise contracts and is unrealistic in particular for bespoke services which involve upfront investment by the enterprise or cloud service provider. Moreover, the onus on the donor to support switching misses the important role that must be played by the recipient provider, as well as the customer in what is typically (in the case of enterprise migration) a project-based exercise. An option for 30 day contract termination may be more realistic for standardised SaaS solutions provided to consumers and small businesses, but requiring this as the only option, could limit the potential for customers to benefit from discounts for engaging in longer contract periods (e.g. of one year), and service continuity may still not be feasible when “switching” due to differences in service characteristics.
- The draft Data Act seems to presume that regulatory intervention is generally necessary to support interoperability and porting in cloud computing but there may not always be a demand for these attributes and where there are demands for specific aspects of interoperability or portability, these are often addressed by the market through voluntarily adopted standardised formats and languages, conversion or migration tools.

In light of these observations, we have made the following recommendations.

Recommendation	Comment
Recommendation 1: Targeted (case specific) intervention rather than general obligations	Instead of blanket obligations for cloud interoperability and portability and undefined standards goals, clarify that the Commission can intervene to request standards development and/or mandate given standards for specific applications/cases where there is an objective interest based on evidence of demand for a specific form of interoperability and/or portability that is not being met by the market., and the conditions described in Recommendation 2 are met
Recommendation 2: Support for innovation, respect for proportionality	When considering the development and potential mandating of standards relating to cloud computing, ensure that the relevant use cases are clearly identified, intervention is relevant to the problem identified, and that the measures are proportionate and take into account the implications on innovation and the potential to differentiate. Limit the objective that interoperability should achieve “functional equivalence” to basic functions and/or data (i.e. a subset of mature and established functions or data which have been identified as essential), and further clarify this concept.
Recommendation 3: Principles for service migration and shared responsibility	As regards switching: in place of the unrealistic and indiscriminate requirement to offer contract termination within 30 days at no cost, and with assurance of service continuity, require cloud service providers to collaborate in good faith to facilitate porting of customer data and applications in the context of service migration. An option for 30 day contract termination could also be provided specifically for standardised SaaS solutions provided to consumers and small businesses but should not be mandatory (as customers may prefer other options). Support for migration could also be offered to CSPs and their customers (in particular SMEs) by developing model contract provisions addressing certain common issues.
Recommendation 4: Coherence with other legislation	The Data Act should avoid overlapping or adding to other legislative measures. It should focus on procedures to implement symmetric measures which are not already addressed through other symmetric instruments, or through asymmetric obligations applied under the DMA. Standardisation should involve participation and commitment from relevant sectors as a whole

2 Introduction

Cloud computing is an important enabler for the digital economy. In addition to reducing costs, and transferring capital expenditure to operational expenditure, cloud computing can improve access to advanced IT solutions such as High Performance Computing and AI capabilities, boosting innovation[7] and productivity across a wide range of sectors,[8] which is vital in supporting sustainable growth and recovery following the challenges of COVID and the energy crisis. In its vision for Europe's Digital Decade,[9] the European Commission has established a target that 75% of EU companies should make use of technologies such as cloud computing, AI and big data.

As cloud computing has gained momentum, there has also been an increasing focus on governance issues relating to cloud computing, the need to ensure that customers can make use of multiple services and are not locked into their cloud provider(s), and that providers of cloud computing services that are found to be "gatekeepers" do not exploit this position to undermine fairness and contestability. These concerns underlie the adoption of certain provisions in the Digital Markets Act,[10] as well as proposals in the draft Data Act,[11] concerning cloud interoperability and portability.

The concepts of interoperability and portability are not new, even in the emerging cloud computing ecosystem, and have been well-described through ISO/IEC standards.[12] Furthermore there are well-established examples of regulatory requirements relating to interoperability and portability in other sectors, notably telecoms and banking, as well as interoperable services that have emerged "by design" such as email. However, the application of regulatory requirements on interoperability and portability to the cloud requires further analysis as the services and possible scenarios for interoperability and porting are significantly more complex than in the cases where these concepts have been mandated in the past and the problems, causes and implications of specific solutions to address lock-in concerns linked to cloud computing (including unintended consequences) may not have been adequately described.

7 Carlos Moedas, Commissioner for Research, Science and Innovation, noted in May 2018 that „The Cloud will be a game changer for science in Europe." European Commission, Directorate-General for Research and Innovation, Horizon Europe : strategic plan 2021-2024, Publications Office, 2021, https://data.europa.eu/doi/10.2777/083753

8 Various studies have highlighted the potential for cloud computing to boost productivity across the wider economy See for example LSE (2019 https://www.lse.ac.uk/business/consulting/reports/the-transformative-effect-of-cloud-on-firm-productivity-and-performance#:~:text=This%20research%20indicates%20that%20cloud,%2C%20location%2C%20size%20or%20sector

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

10 https://www.europarl.europa.eu/doceo/document/TA-9-2022-0270_EN.html

11 https://digital-strategy.ec.europa.eu/en/library/data-act-proposal-regulation-harmonised-rules-fair-access-and-use-data

12 https://www.iso.org/standard/66674.html

This study seeks to provide guidance on what is meant by cloud computing services, and what is meant by interoperability and portability. We describe how these concepts have been applied in other sectors, in which circumstances they may be relevant to cloud computing, the benefits and risks (including potential implications for differentiation and innovation) and what might be the implications for the ongoing review of the Data Act. The study is structured as follows:

- Chapter 3 defines cloud computing and discusses different use cases
- In chapter 4, we discuss what is meant by interoperability and portability and how it has been applied in other sectors
- Chapter 5 identifies scenarios where portability and/or interoperability may be relevant in the context of cloud computing; and
- Chapter 6 discusses the implications of our analysis for proposed legislative measures relating to the cloud, and makes recommendations on this basis

3 What is cloud computing and how is it used?

This chapter introduces the used terms for cloud computing in this report, discusses how the cloud market is evolving, who are the main suppliers and what are the competitive dynamics.

- Cloud computing is the delivery of computing services—including servers, storage, databases, networking, software, analytics, and intelligence—over the Internet. It offers an **alternative for customers deploying their own, on-premises IT infrastructure**, and in doing so saves cost (and in particular capex) as well as offering **access to state-of-the-art hardware and applications** that customers would otherwise not be able to replicate.
- Cloud services have traditionally been categorised into **Infrastructure as a Service (IaaS)**, **Platform as a Service (PaaS) and Software as a Service (SaaS)**. These categories reflect the division of responsibility between the customer and the cloud provider. However, the demarcation between IaaS and PaaS is rather fluid. With IaaS, customers outsource their physical IT infrastructure like storage, network and data centres. PaaS offers a platform for developing applications. SaaS refers to the remote provision of applications.
- Whereas a **private or dedicated** cloud is deployed by or for a specific customer, **public** cloud serves multiple customers, bringing benefits in flexibility and cost. These economies of scale apply even more to so called **hyperscalers** involving hundreds of thousands of servers in datacentres across the globe.
- Customers can use multiple public clouds to access the same or different applications. These are called **multi-cloud** solutions. When private and public cloud services are mixed, this is referred to as **hybrid cloud** solution. For both options, so-called edge servers can be added to shorten response time for time critical applications, which is called **edge computing**.
- While IaaS and PaaS are used predominantly by developers and IT professionals at enterprises and other organizations to install and/or build their own applications, **SaaS functions as a delivery model for all kinds of services including services which are familiar to consumers** such as remote file storage and back-up, cloud-based productivity tools, video streaming, email and social media.
- **The cloud market is very diverse**, with multiple specialised niches and many different suppliers. Suppliers include Appium, Apple, AWS, Citrix, Google, IBM, Katalon, Microsoft, NetApp, Oracle and PubNub, SAP, Salesforce, Rackspace and Red Hat. On a wide interpretation, enterprise customers that develop and offer services in the cloud could also be said to be cloud providers.

- As of 2021, only **41% of companies in the EU were using cloud computing** and many companies take a conservative approach, opting to combine their own data centre and cloud services. Moreover, a significant proportion of cloud usage is limited to basic services like mail and file storage. Today its use is more prevalent in high tech sectors and smaller companies have on average been slower to embrace cloud. However, it has provided **opportunities for start-ups to scale up and innovate more rapidly**, providing an indication of the benefits that could be achieved through wider diffusion of cloud across the economy.

3.1 What is cloud computing?

Cloud computing enabled on-demand access to a range of computing services

Cloud computing is defined by ISO/IEC as defined as '..a paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand.'[13] It typically involves the provision and billing of IT services dynamically, via a network, so the IT services can be scaled to meet the demands of the customer.[14] As such, cloud computing offers an alternative for companies or individuals to maintaining their own IT systems in-house (or "on-premises"). Cloud computing can cover a diverse range of information technology solutions which can range from the provision of access to infrastructure (e.g. computing power, storage space) to the remote provision of platforms and software.[15] In addition to offering services for the customers' internal use, the cloud can be used as a delivery platform for the provision of online services in general.

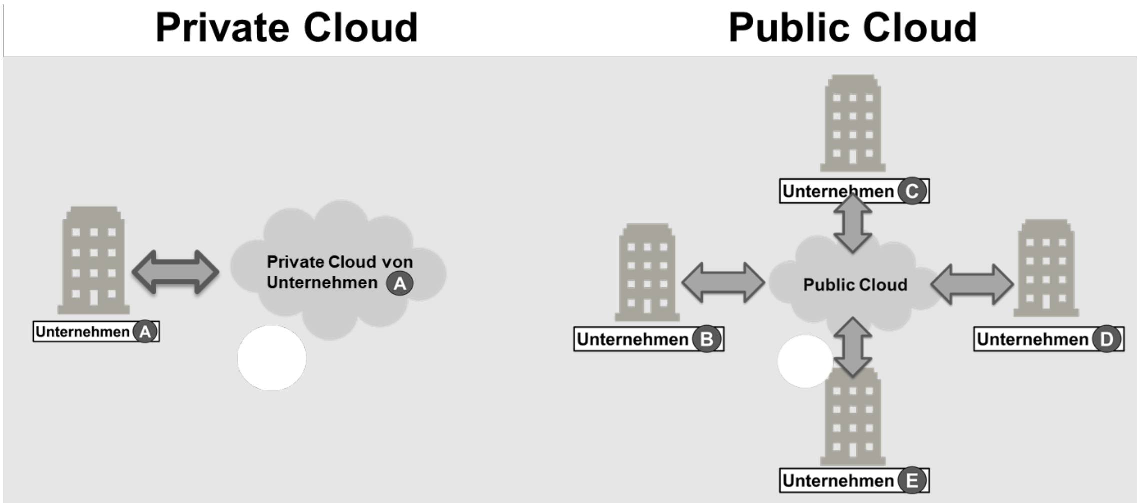
Private, dedicated, public and hyperscale clouds

A cloud service which is operated exclusively for the benefit of a single company or organisation (e.g. remote server farm), can be run by the company itself (private cloud) or an external cloud provider (dedicated cloud). On the other hand, a public cloud is a cloud service offered by a cloud provider to multiple customers.

---

13 ISO/IEC: 19941:2017(E), Information technology — Cloud computing — Interoperability and portability.
14 See definition from German Federal Office for Information Security.
15 Bundesamt für Sicherheit in der Informationstechnik (2020).

Figure 1 Private versus public cloud services



Source: WIK-Consult

One of the traditional benefits of public clouds is that they enable scalability and the sharing of resources, enabling customers to access a wider range of capabilities for lower costs.[16] In addition, the costs are directly related to usage (OPEX) rather than capital expenditures (CAPEX). Furthermore, there is higher flexibility than would be possible for a cloud operated for a single company.[17] Further scalability in service provisioning and economies of scale can be achieved through so-called "hyperscale" cloud solutions, which offer the potential to access a distributed computing environment involving hundreds of thousands of servers in datacentres across the globe. Various studies have indicated that significant cost savings can be made by moving in-house IT systems to the (public) cloud.

In addition to cost saving opportunities, customers can benefit from cloud-native technologies such as orchestration, containerization, and microservices, which enable cloud users to create services faster, and create offers for their customers that were not possible before. This has enabled start-ups to develop and launch applications without the need to own infrastructure. In addition, the concentration of advanced technological

16 For example, Johnson, Callaghan et al (2019) Cost Comparison of an On-Premise IT Solution with a Cloud-Based Solution for Electronic Health Records in a Dental School Clinic found that over a two-year period, both one-time and ongoing costs were higher for the on-premise solution than the cloud-based solution (by 40.5% and 20.5%, respectively). https://pubmed.ncbi.nlm.nih.gov/31010892/#:~:text=The%20overall%20cost%20of%20an,of%20the%20on%2Dpremise%20solution. See also Nayar, K.B. and Kumar, V. (2018) 'Cost benefit analysis of cloud computing in education', Int. J. Business Information Systems, Vol. 27, No. 2, pp.205–221, which refers to a survey at universities moving towards cloud computing having an increased efficiency of 55%, increased mobility 49% and lowered cost 25%. The biggest benefit is however innovation as any organisation can enjoy the latest technologies unlike traditional technologies.

17 In addition to public and private cloud one can also define community cloud, which is shared by companies and/or institutions belonging to one community with a common case (e.g. research institutes).

skills and pooling of resources facilitated by the cloud enables customers to make use of advanced and otherwise costly resources such as high performance computing, AI and big data processing, which they may otherwise not be able to support.

Different layers of the value chain

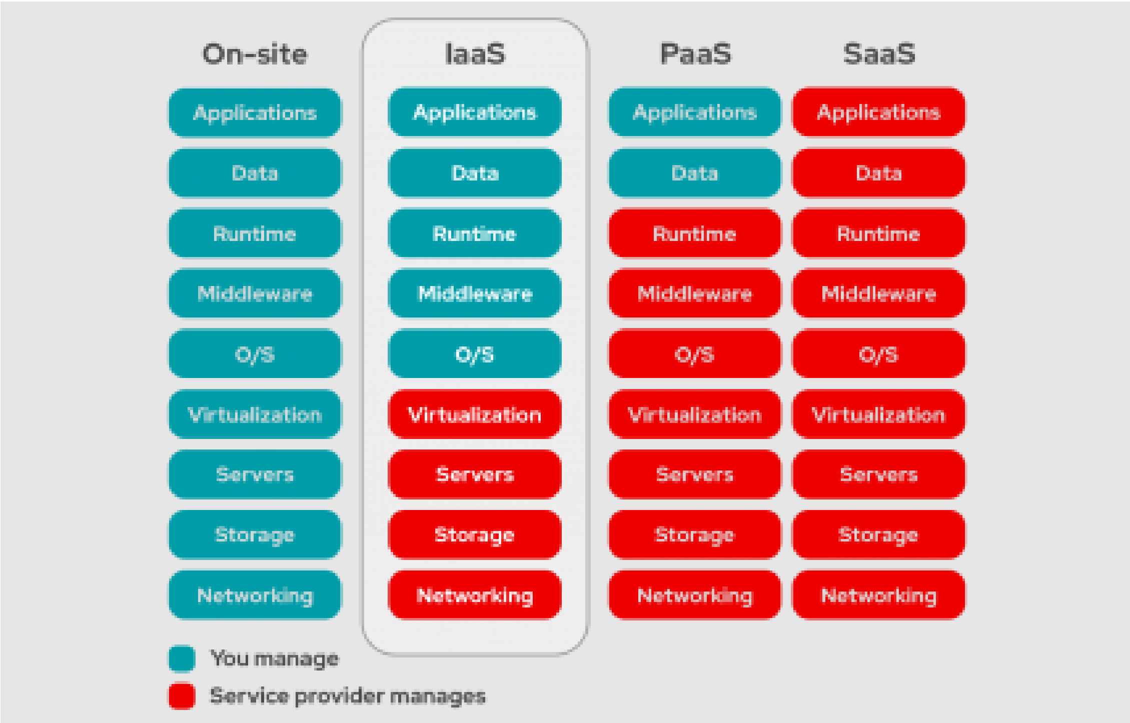
Public cloud provision can be segmented according to how tasks and responsibilities are divided between the customer and the cloud provider. The standard service models are called Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS):[18] [19]

- IaaS includes IT resources such as computing power, storage, networks or the virtualisation of hardware. This service is used in particular by company's IT administrators.
- PaaS offers a platform with standardised interfaces is offered to develop and run the company's own applications. This service is mostly used by software developers.
- SaaS offers scalable online-capable standard applications. These services target end users.

An illustration of the division of responsibility based on these cloud categories is shown in the following figure.

18 Bundesamt für Sicherheit in der Informationstechnik (2020), KPMG (2021), Page 14.
19 Bundesamt für Sicherheit in der Informationstechnik (2020), Haselmann et al. (2012), Page 30.

Figure 2 Service models of public cloud services



Source: https://azure.microsoft.com/en-us/overview/what-is-cloud-computing/#benefits

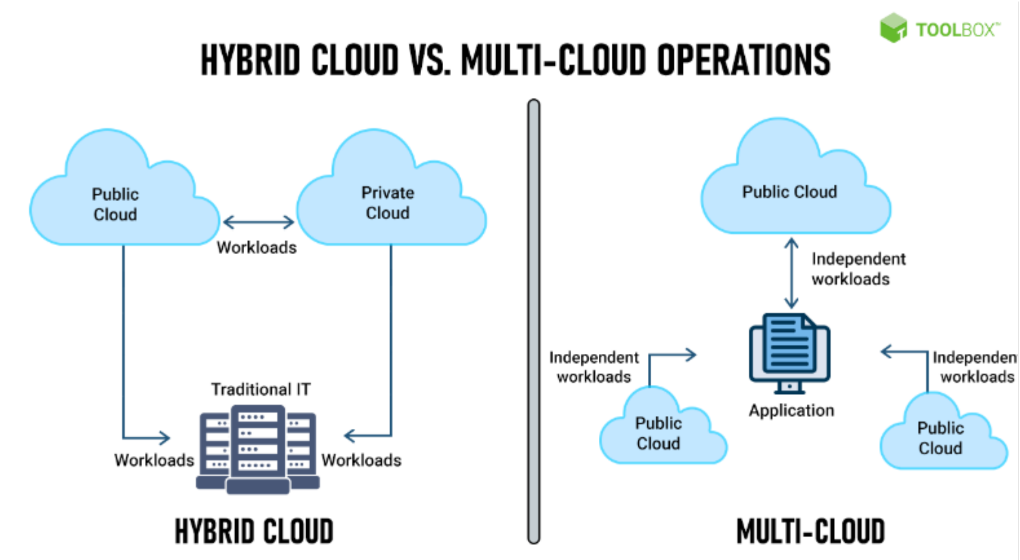
It should be noted however that as these categories were specified around 2012, new offerings have developed based on the ‘as a service’ model including Network as a service, Data as a service and Container as a service. The demarcation points between IaaS and PaaS in particular are thus not clear-cut.

Multi, Hybrid and Edge Cloud solutions

Multi cloud solutions consist of more than one cloud solution of the same type (public or private) from different cloud providers. Hybrid cloud, on the other hand, involves the use of several clouds of different types (public and private cloud).[20]

20 Red Hat (2021).

Figure 3 Hybrid versus multi cloud services

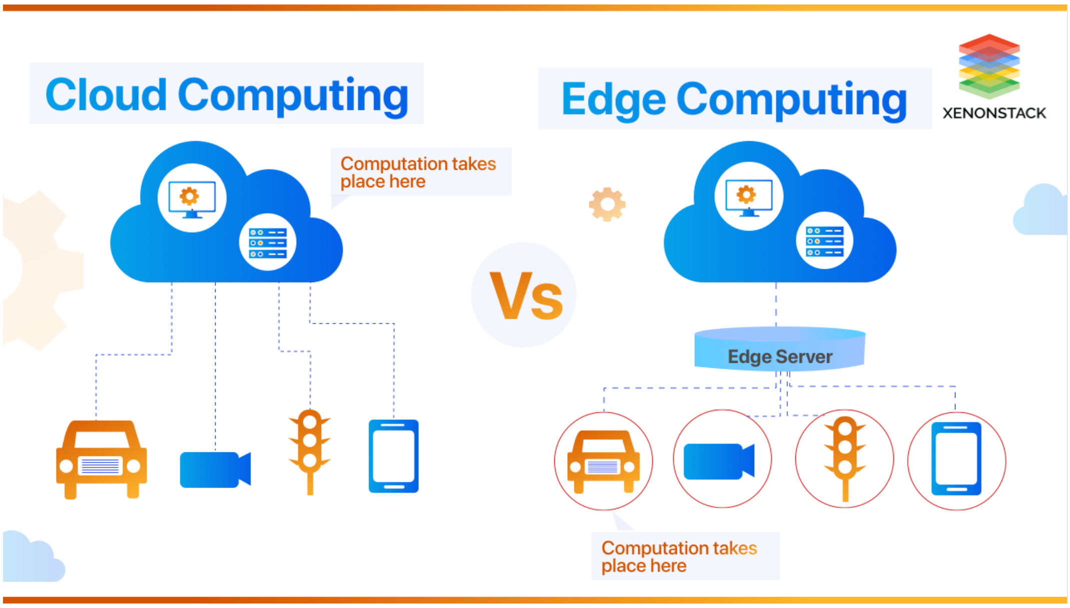


Source: Toolbox.com[21] and RedHat
https://www.redhat.com/en/topics/cloud-computing/public-cloud-vs-private-cloud-and-hybrid-cloud

Edge cloud refers to developments to bring the functionality and accessibility of the cloud closer to the place where the data is generated, stored, processed and used (the network edge). This is done to shorten response times for time-critical applications, save costs for data transmission or to keep sensitive data closer to the source.[22] Edge cloud computing particularly addresses the growing market of industrial IoT[23] applications where real-time computing power is required.

21 https://www.toolbox.com/tech/cloud/articles/multi-cloud-vs-hybrid-cloud/
22 Intel (2021).
23 Internet of Things

Figure 4 Cloud services and adaptations for edge computing

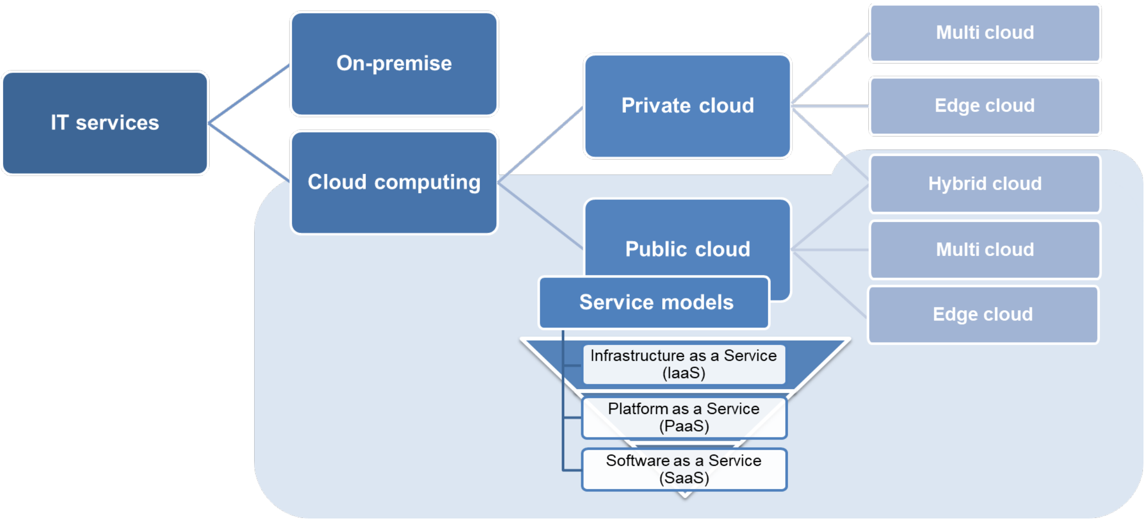


Source: Xenonstack

Overview of cloud computing solutions

The following diagram provides an overview of the different IT options available to corporate customers.

Figure 5 Overview of Cloud Computing

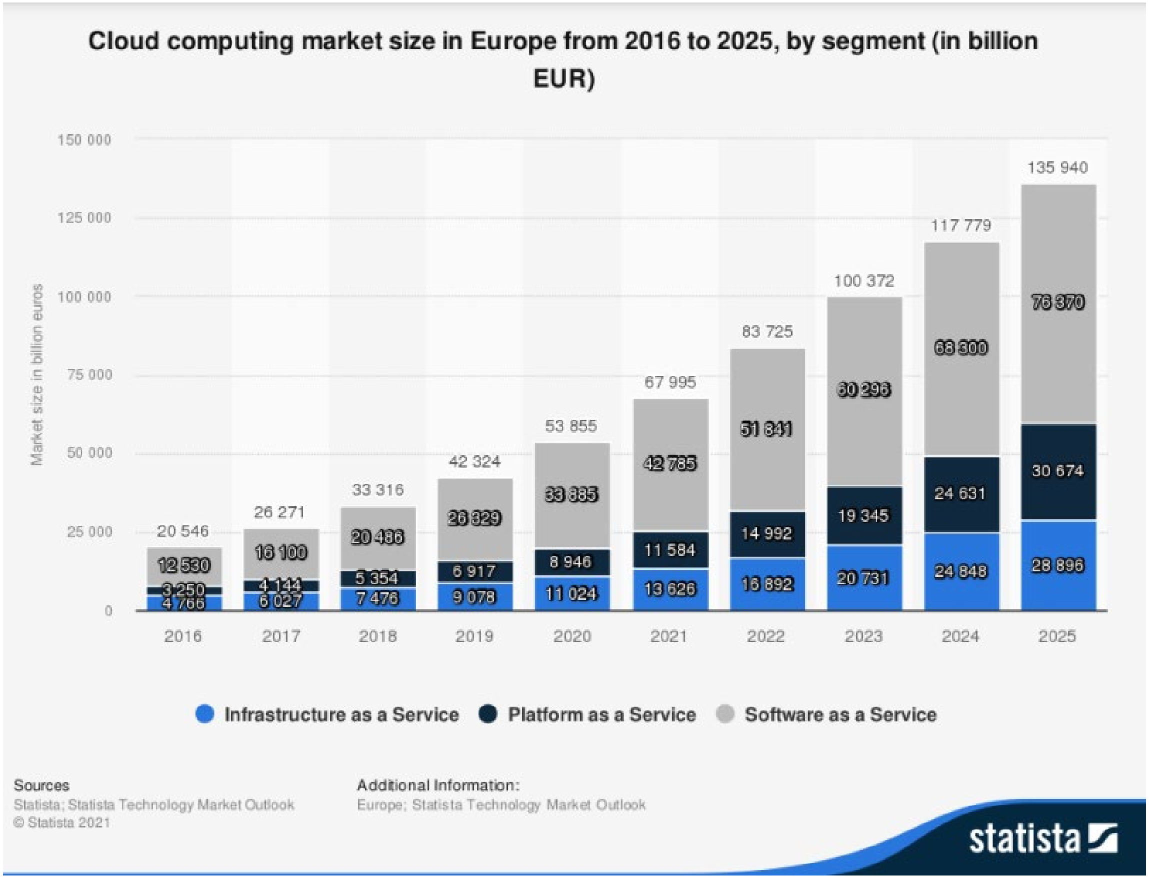


Source: WIK-Consult

3.2 How is the market evolving?

The cloud computing market in Europe was estimated at around €68bln in 2021. Although all elements of the cloud value chain are expected to expand in the coming years, PaaS is expected to achieve the most significant growth.

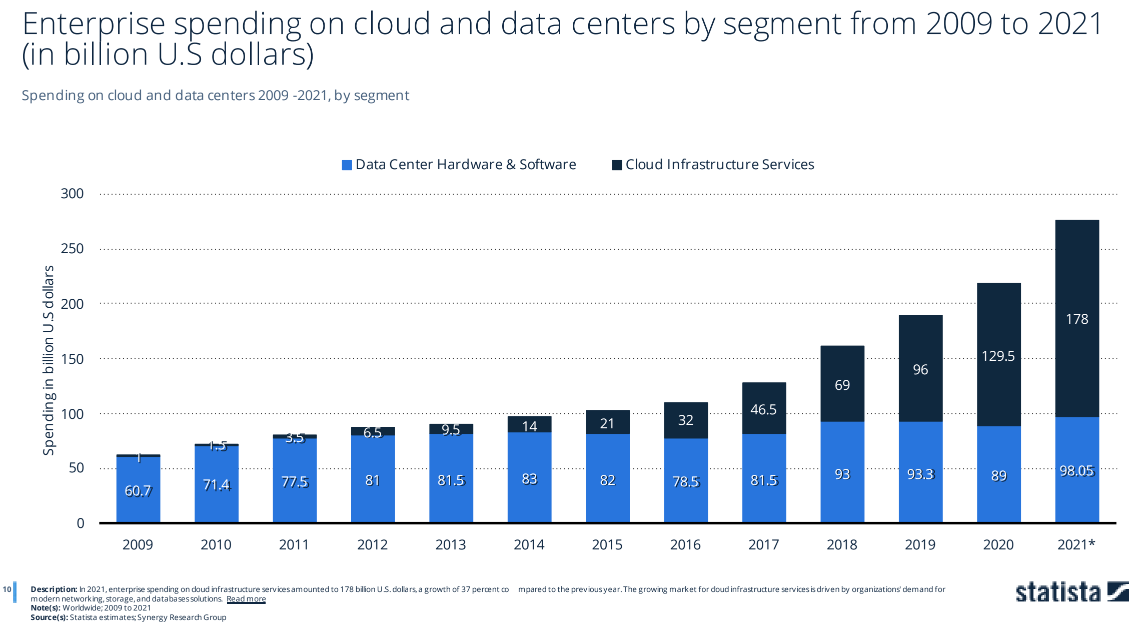
Figure 6 Revenue Cloud services in Europe 2016 – 2025 (prior trends and forecast)



Source: Statista (2022)

Although companies could in principle replace their on-premises hardware and rely exclusively on the cloud, data suggests that at the moment, companies often maintain their on-premise data centres to perform complementary tasks or provide back-up. Thus, spending on cloud solutions has largely been additive.

Figure 7 Enterprise spending worldwide 2009-2021: data centre (on-premise) versus cloud



Source: Statista

Who is using cloud computing and what do they use it for?

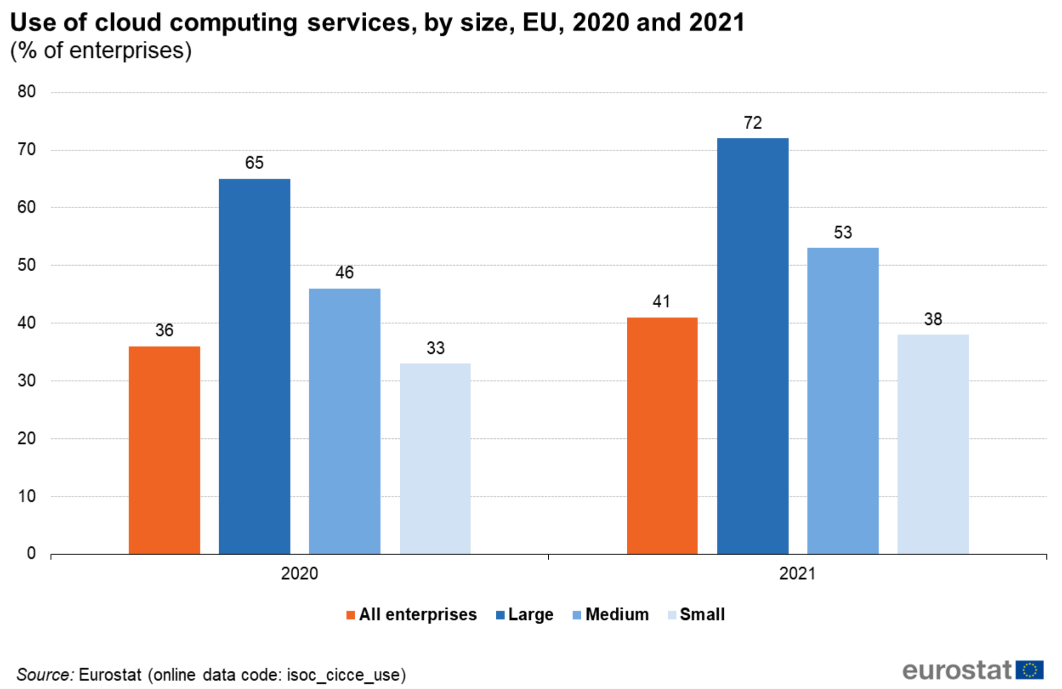
According to data from Eurostat, on average, 41% of companies with ten or more employees in the 27 Member States of the European Union (EU) used cloud computing in 2021, 5% higher than in the previous year.[24] However, this figure conceals wide disparities across different countries.

While Sweden, Finland (75 %), the Netherlands and Denmark (65%) all have high usage of cloud services, the diffusion of cloud computing is less advanced in Greece (22%), Romania (14%) and Bulgaria (13%).

Cloud usage is also more prevalent in larger companies. For example, in Germany 24 % of SME companies (< 9 employees) relied on cloud computing in 2020 while 62% of large companies (>250 employees) made use of cloud computing services. [25] A similar pattern can be seen in the EU as a whole (see following figure). However, cloud services have also helped start-ups to launch and scale up more rapidly and provided a platform for dynamic companies to innovate.[26]

24 https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Cloud_computing_-_statistics_on_the_use_by_enterprises
25 German Bureau of statistic (DESTATIS), Press announcement 241, 21 May 2021, https://www.destatis.de/DE/Presse/Pressemitteilungen/2021/05/PD21_241_52911.html
26 See for example https://www.researchgate.net/publication/316069451_Analyzing_Cloud-based_Startups_Evidence_from_a_Case_Study_in_Italy

Figure 8 Use of cloud computing by size of company in 2020/21



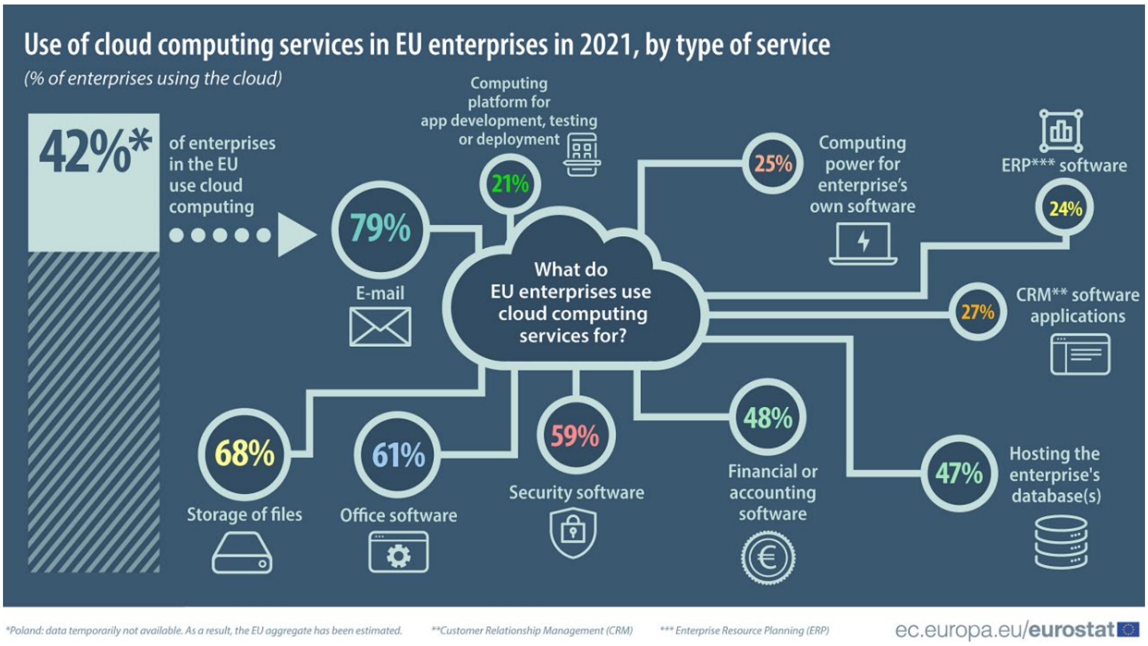
Source: Eurostat

There are disparities between take-up of cloud by different sectors, with higher uptake in ICT and professional, scientific and technical industries than in sectors such as manufacturing.[27]

It should also be noted that a high proportion of cloud use is still related to more basic services such as email and file storage, and the use of cloud for more "advanced" applications such as ERP and CRM software is more limited. This means that customers are not yet reaping the full benefits (and productivity gains) that could be achieved through a more advanced use of cloud services.

27 https://ec.europa.eu/eurostat/statistics-explained/index.php?title=File:Use_of_cloud_computing_services,_by_economic_activity,_EU,_2020_and_2021_(%25_of_enterprises)_v2.png

Figure 9 Use of cloud computing services in EU enterprises in 2021, by type of service



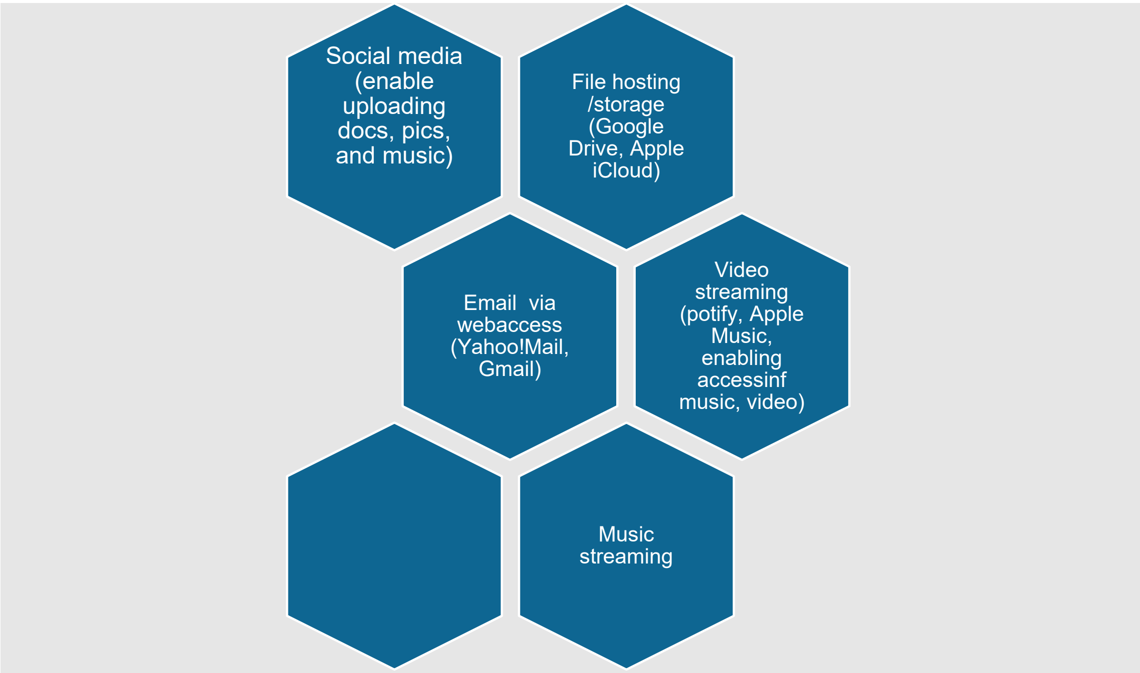
Source: Eurostat

Consumer cloud

Although cloud is often thought of as a business application, consumers are also increasingly making use of "Software as a Service". Document exchange services such as Dropbox, content lockers and video streaming services such as Netflix or iTunes, cloud back-up solutions such as iCloud, ecommerce and social media provide just a few examples of consumer-facing services which are typically based in the cloud. See following diagram for examples in different areas.[28]

28 See [What Is 'the Cloud' — and How Can Consumers Use It? - FTC]

Figure 10 Software as a Service examples



Source: WIK

3.3 Who are the main suppliers and what are the competitive dynamics?

<u>Service providers of cloud solutions and use cases</u>

Cloud computing covers a very diverse set of services. There are a variety of suppliers active at the different levels of the value chain, some of which provide comparable services while others operate in a specific niche.

The following tables provide a few examples of the services provided for different use cases.

SaaS

Service categories	Main providers (service name)	Customers	Used for?
Online Mail	Apple (iCloud Mail) Google (Gmail) Yahoo (Yahoo!Mail) Microsoft (Outlook.com)	residential customers	personal email handling at any location
Office applications via web interface	Microsoft (Microsoft 365), Google (Works, Docs, Spreadsheet, Word processor) IBM (LotusLive)	Business & residential customers	office automation (mail, word processing, spreadsheet, presentations, conferencing etc.)
Customer Relation Management (CRM) via web interface	Salesforce (Sales Cloud) Microsoft (Dynamics 365) Zoho CRM Monday.com /Sugar CRM / Oracle (Netsuite) / SAP CRM (Service Cloud) etc.	business customers; large enterprises started first using CRM tools but also more and more SME.	Integrated support for all customer facing activities of companies. Including among others: contact and lead management, workflow automation, predictive sales and analysis, marketing automation tools
Data Management Systems via web interface	IDrive MS (OneDrive) Dropbox (Business Sync/Backblaze	Specific business solutions and separate ones for residential customers	Backup/Restore of data in the cloud and online access at any place
Enterprise Resource Planning (ERP) systems via web interface	SAP (SAP S/HANA) Oracle (JD Edwards Enterprise One, Netsuite) Microsoft (Dynamics 365) And more	Business customers	Supporting business processes by linking them (order entry, stock management, procurement, production)
Virtual desktop via web interface	NetApp (Virtual Desktop Service) Citrix (Virtual Apps and Desktops) / Itopia / VMware / Workspot based on Google Cloud MS Azure Virtual desktop	Business customers	Enabling the shift from traditional desktop model to a virtual desktop in the cloud enabling access for end users at any location.
Blog websites	Allthatsaas.com Saasmetrics.co Crazyegg.com/blog/ https://blog.hubspot.com/	Business customers	Providing information on the use of SaaS via a website with regular updates (a blog).Part of SaaS marketing strategy
SaaS application testing	Appium Katalon TestProject Postman Etc.		Supports the testing and validation of SaaS applications (on functions, load handling, performance, interoperability and GUI). Speeds up the product development.

PaaS

Service categories	Main providers (service name)	Customers	Used for?
General purpose	Infinite Blue platform (previously Rollbase) Software AG (LongJump)- standard developpers suite Salesforce (App Cloud) Google App engine MS Azure Cloud PaaS / App Service / Cognitive Search AWS Elastic Beanstalk IBM Cloud Pak for Applications	Software vendors Large business customers such as AT&T, Nielsen and Cisco.	Offering a platform to software vendors enabling their application to be offered as a SaaS to end customers. Building and deploying apps in the cloud. Create and deploy traditional applications that offer a 'lift and shift' approach for migration
Support for advanced technologies	Red Hat OpenShift AWS Machine Learning AWS Lambda (serverless PaaS)	Developers	PaaS offerings based on new technologies such as serverless, distributed event processing, machine learning etc.
Specialised	PubNub (provides APIs for real-time development, (eg integrating messaging and social services on apps and websites) Restlet (opensource API framework, visual design tool).		Focuses on developing applications for niche use cases for which there is a high demand

IaaS

Service categories	Main providers (service name)	Customers	Used for?
Virtual Machines (VMs)	AWS VMware Joyent Rackspace	IT / system managers	Create platforms for service and application tests, development, integration and deployment
Message queues	IBM MQ Ms Azure Message Queue		Message queue enable cloud based applications to communicate with each other or with on-premises systems.
Networks	Ionos Software Defined Networking (Compute Engine)		Access to server and network structures in the cloud with flexibility and no configuration or complexity.
Storage/ back up services	AWS elastic computing cloud Google cloud storage Azure ?		Extension of online storage
CPU/memory	Google compute engine AWS Lightsail (virtual private servers)		

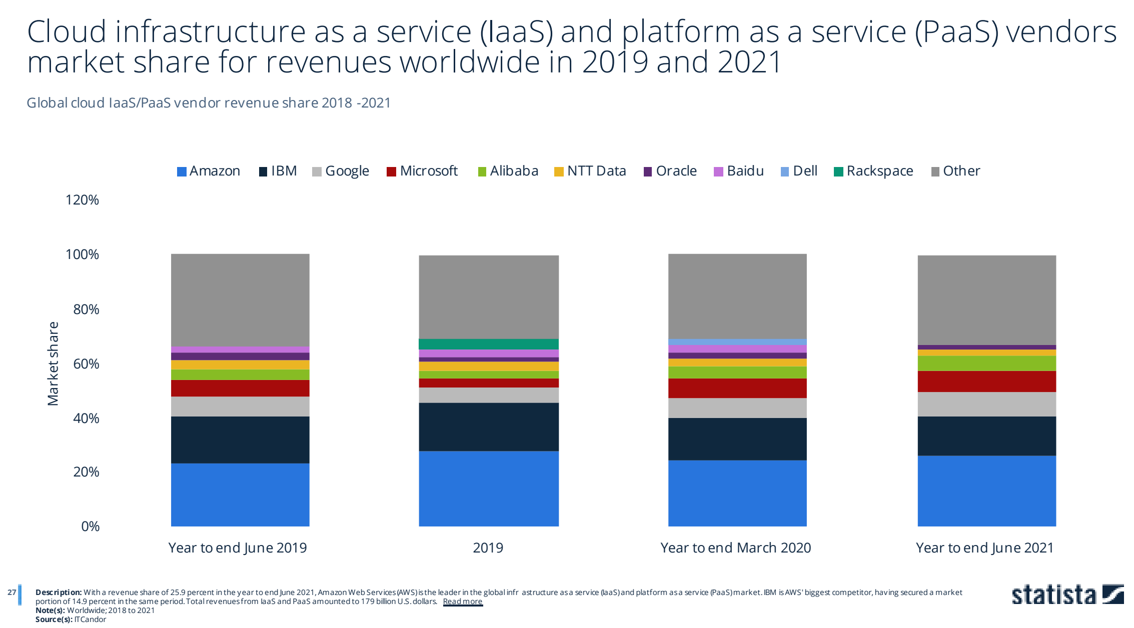
Main suppliers of cloud services and their offerings

The market dynamics and main players in different layers of the cloud value chain differ.

IaaS and PaaS

On a global basis, AWS and IBM hold the leading position in IaaS and PaaS with smaller shares for Microsoft Azure and Google Cloud Platform. European providers such as Deutsche Telekom, OVH, Orange and Swisscom are also present in this space and have more than doubled their revenues in the past four years, although from a low base.[29][30]

Figure 11 Cloud infrastructure as a service (IaaS) and platform as a service (PaaS) vendors' market share (worldwide revenues in 2019 and 2021)



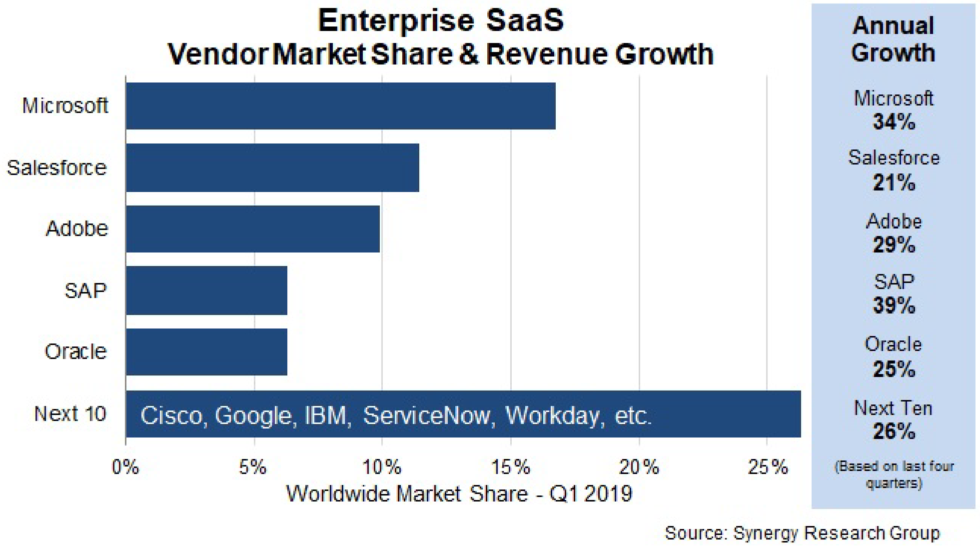
Source: Statista

SaaS

SaaS is a diverse segment featuring a number of different players including Microsoft, Salesforce, SAP and others. Services evolve rapidly and are adapted to different use cases. The following figure shows some of the actors present in the enterprise SaaS segment. 5 players have a significant share in this market with significant growth from players such as SAP as well as Microsoft and Adobe. Other players including Google, IBM and ServiceNow are also present in this segment.

29 Synergy Research Group (2020a).
30 Synergy Research Group (2021b).

Figure 12 Enterprise SaaS-revenue share and growth



Source: Synergy Research Group

It should be noted however that even in this segment products differ, and comparisons become even more challenging amongst the wide variety of other use cases for SaaS.

For example, in its widest interpretation, many enterprise customers which develop platforms or services based on IaaS or PaaS which they offer to the public could be viewed as SaaS providers.

4 How has interoperability and portability been applied in other contexts and in which contexts has it worked?

In this chapter, we consider the meaning of interoperability and portability and discuss how it has been applied in other contexts in the digital economy including electronic communications, online banking and email. We conclude by identifying lessons from other sectors and common factors that contribute to identifying successful applications of interoperability and portability. Key findings are shown below.

- **Interoperability refers to the degree to which two or more systems, products or components can exchange information** and make use of the information exchanged. It is possible to identify **different degrees of interoperability**, from no interoperability to full interoperability. **Horizontal interoperability** refers to communication between two systems at the same level of the value chain, while **vertical interoperability** refers to interaction at different levels of the value chain e.g. to develop applications on a platform, or add-ons to software.

- **Portability refers to the potential to export or transfer data, applications or platforms** from one IT system to another. This potential might vary but will often not be 100% because applications and underlying IT systems will always have certain differences. **Portability generally refers to a one-time transaction, whereas interoperability is continuous.**

- **Switchability** is a non-legal and non-technical term and generally used to refer to the ease with which end-users can switch from one service or system to another. It could involve, alongside the porting of any required data or applications, **the ease of terminating the contract** with one party and subscribing with another (and associated timeframe and cost). Switching implies that the new service provides similar basic functionality as the old service i.e. that it is viewed from the customers' perspective as a substitute.

- A common feature that can be seen in the development of (horizontal) interoperability e.g. in telecoms and email, is that the **process took time**, and involved **standardisation of specific features that form essential (and common) components** in these vital services (e.g. signalling and call routing in the case of telephony, protocol and addressing in the case of email). Once standardised, there was **little further innovation** in these basic services. Non-standardised innovative services such as messaging and communication via social media evolved in parallel and have to a certain extent overtaken some of the basic functions that used to be performed such as voice calls and SMS. There have been efforts to create standardised versions of more feature-rich messaging services, such as MMS and subsequently RCS, however these features have been developed with a significant time lag, and it is not clear to what extent consumers will embrace them.

- These examples show that interoperability can be a powerful tool in delivering any-to-any communication. However, key lessons are that while the measures can be vital to create a baseline of essential interoperable services, **innovation mainly occurs beyond those services as standardisation tends to halt the evolution of services which are captured by those standards.**

- Open banking provides an example of vertical interoperability whereby certain essential, commonly understood features of banking services such as identifiers, transaction details were opened up to application developers, which could take the opportunity to develop add-on services such as analysis of transaction patterns (to identify fraud) or develop platforms where consumers could access information from multiple banks. A key feature is that it was applied to an essential service, and focuses on key, but basic data inputs and formats. The proposals for a European Digital Health Space is based on a similar premise.

- Portability obligations exist in both telecoms and banking in connection with switching. In telecoms, the focus is on the identifier (number portability), while in banking it includes the transfer of information about recurring transactions and the account balance. In both cases, the concept of portability includes an elaboration of the process (and associated timescale). For banking, in addition, all the transactions associated with the old provider are also ‚ported' to the new provider.

- Portability obligations and deadlines have been essential measures to support switching in telephony and banking. However **portability obligations have been applied to essential services, have focused on relatively simple, basic and limited datasets such as identifiers, and have been used in industries where consumers typically have one single service provider**. This contrasts with cloud computing where services and business models are diverse, applications and related datasets complex and multiple service providers are common both amongst enterprises and consumers.

4.1 What does interoperability mean?

<u>How is interoperability defined?</u>

Interoperability (IOP) can be broadly defined as the ability of two or more software components to work together despite differences in language, interface and execution platform (Wegner, 1996, p. 1) [31]

31 Wegner, P. (1996). Interoperability. *ACM Computing Surveys (CSUR), 28*(1), 285-287.

More specifically, interoperability is defined in the ISO/IEC/IEEE Directory of System and Software Engineering Terms (ISO, 2017, p. 237) as "the degree to which two or more systems, products or components can exchange information and make use of the information exchanged" and "the ability of objects to cooperate, i.e. the **ability to communicate information to each other** in order to exchange events, proposals, requests, results, commitments and flows". [32]

Different degrees of interoperability

The degree of interoperability may vary depending on the scope; for example a subset of all functionalities provided by a specific application may be interoperable with other applications, while the remaining functions are only available to the users of the corresponding application itself. Chou & Shy (1993) called this partial IOP, which suggests a **continuum from "full interoperability" to "no interoperability"**.[33] The degree to which interoperability can be achieved between applications is also be affected by the degree to which data and functions in one application are relevant for the other, as interoperability is only meaningful for data and functions which play a similar role (i.e. it is context dependent).

Horizontal and vertical IOP

Riley (2020) [34] distinguishes **horizontal** (between comparable services) and **vertical** interoperability (between services up- and downstream of one another in the value chain).

The case of horizontal IOP describes, for example, IOP between comparable messenger services. Vertical IOP relates for example to the seamless cooperation of a payment service with an e-commerce platform. The important aspect is whether the services are in direct competition with each other (messenger example) or function as an upstream or downstream add-on to for example an e-commerce platform, which thereby positively influences the competition position of the e-commerce platform. (Jacobides & Lianos, 2021b).[35]

---

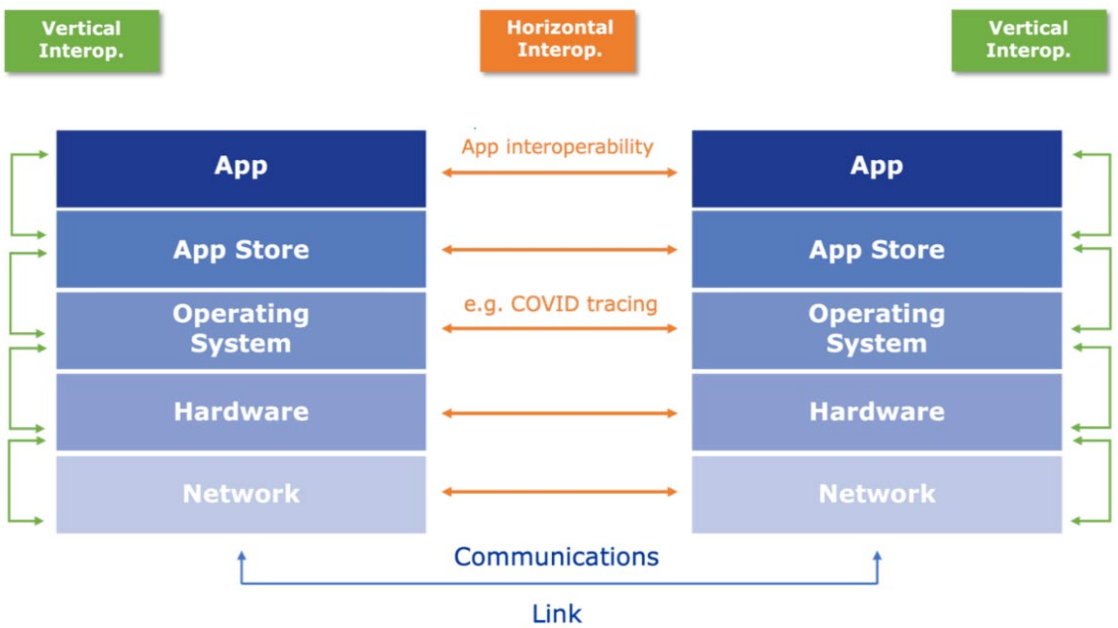
32 ISO (2017). iec/ieee international standard-systems and software engineering–vocabulary. *ISO/IEC/IEEE 24765: 2017 (E)*.

33 Chou, C.-f., & Shy, O. (1993). Partial compatibility and supporting services. *Economics Letters, 41*(2), 193-197.

34 Riley, C. (2020). Unpacking interoperability in competition. *Journal of Cyber Policy, 5*(1), 94-106.

35 Jacobides, M. G., & Lianos, I. (2021b). Regulating platforms and ecosystems: an introduction. *30*(5), 1131-1142.

Figure 13: Horizontal and vertical IOP in mobile Ecosystems



Source: Bourreau, Krämer, & Buiten (2022, p. 15)

Vertical interoperability is enabled via technical interfaces (APIs) and aims to stimulate innovation by complementary providers (to the digital platform). Vertical interoperability is always asymmetric, as the aim is for the platform to grant unilateral access to third-party providers to innovate "over-the-top" (Bourreau et al. 2022),[36] without altering the service characteristics or undermining the security features of the underlying platform.

Horizontal interoperability is enabled by adhering to certain standards and/or providing open interfaces, which reflect the current state of innovation.

Horizontal interoperability can be symmetrical or asymmetrical. With one-way (asymmetric) IOP, it is possible to transfer information directionally to or from an application. Symmetric IOP would be the two-way exchange between users of different applications and services (Manenti & Somma, 2008). [37]

36 Bourreau, M., Krämer, J., & Buiten, M. (2022). *Interoperability in Digital Markets*.
37 Manenti, F. M., & Somma, E. (2008). One-way compatibility, two-way compatibility and entry in network industries. International Journal of the Economics of Business, 15(3), 301-322.

4.2 What is meant by portability and how does it relate to switchability?

What is the meaning of portability?

Portability refers to the ease with which it is possible to export or transfer data, applications or platforms from one IT system to another.[38] Portability generally refers to a one-time transfer, whereas interoperability could be seen as a continuous transfer or exchange of information between two systems.

Data and application portability

Data portability refers to the selective export of data from an application or a service, which is available for import when switching to another service. Data portability is also possible for services that are not interoperable but requires at least an exchange capability.[39] The ported data can involve identifiers, data created by the user, transactional data (i.e. data relating to the activities undertaken by the user) or data inferred about the user from analysis of his or her transactions.

Porting of applications refers to the migration of applications and associated data from an on-site server farm to the cloud (or from one cloud to another). The degree to which direct porting can be achieved depends on the compatibility of the underlying platform.

Portability vs switchability

Switchability is not a technical or legally defined term, but in contexts where switching obligations apply, the concept generally refers to the ease with which end-users can switch from one service or system to another e.g. in relation to timeframe and cost. In practice, switching is likely to involve, alongside the technical aspects of data and/or application porting contractual aspects (ease of terminating the contract with one party and subscribing with another), compliance aspects (certification, audit, business continuity issues) as well as organisational aspects (change of business processes).

4.3 Applications of interoperability and portability in other sectors

Interoperability and portability have been implemented in other sectors, including fixed and mobile telecommunications and banking. Interoperability is also a core inbuilt feature of the basic Internet application email. In the following sections, we provide an overview of the kinds of interoperability and portability that have been applied in these sectors and services, the timeframes involved in implementation, and the implications for innovation. We conclude with an overview highlighting lessons learned and the degree to which these

38 https://www.techopedia.com/definition/8921/portability
39 Krämer, J., P. Senellart, & de Streel, A. (2020). Making data Portability More Effective for The Digital Economy, Centre on Regulation in Europe (CERRE) Report, https://cerre.eu/publications/reportmaking-data-portability-more-effective-digital-economy/

cases are relevant to the debate regarding interoperability and portability in the context of cloud computing.

4.3.1 Electronic communications

Interoperability has been used since the beginning of mobile and fixed telecommunication networks to enable the exchange of highly standardised voice communication and data (SMS/MMS) messages. It emerged to enable customers of different telecommunication providers to reach one another and exchange information – i.e. a form of **horizontal interoperability**. Telecom interoperability has a long history and is rooted in standards set by standards associations like ETSI. As consequence of the high degree of standardisation, there has not been much innovation or change in these basic telephone services.

In parallel, non-standardised innovative messaging and video conferencing services such as Skype, WhatsApp, Telegram and FB messenger have developed and taken the world by storm. These so-called Number independent Interpersonal Communication Services (NIICS) have from the customer view, complemented and/or even replaced traditional telecom voice and data services. In response to these innovations in "over-the-top" communication services, the telecom industry developed an interoperable standard for so-called Rich Communication Services (RCS), which seeks to incorporate some of the innovative services associated with NIICS while being interoperable, implying that certain set of common functionalities must be defined.

In the following paragraphs, we will see that for the telecommunications sector it took considerable effort over multiple years from regulatory and standardisation bodies to achieve interoperability for services like voice calling, short and media messaging, their successor rich communication services and number portability. A common theme is furthermore that these services have not really changed or expanded much in functionality over time since as this would require expanding the standards and implementation to maintain interoperability. In addition, for number portability we note that obligations apply on both on the donor and the recipient operator to facilitate the process of number porting and consequent migration of the customer from one service provider to another.

<u>Voice and data interoperability</u>

Until market liberalisation at the end of the 1990s, most telephone connections were operated by state monopolies. Their task was in particular to ensure IOP between fixed and mobile lines and with international numbers. At that time, international IOP in particular, was a commercial decision made by state-owned companies, which made it possible to achieve high margins for international connections.

As early as 1983, work started on a European standard for mobile voice telecommunication, but it took until 1987 to produce the first GSM technical specification, which enabled interoperability among those operators using this standard.[40]

Market liberalisation created new challenges as new operators entered the fixed and mobile telecommunications markets and IOP had to be established between the new and existing telecommunications networks. These challenges required a significant amount of legislation and standardisation over the years by national regulators, the European Commission and other international organisations and bodies, in particular the International Telecommunications Union (ITU) and the European Telecommunications Standards Institute (ETSI). As a result of all these regulations and standards, an ecosystem of interoperable networks and services gradually emerged.

The legislative background included several EU Directives which sought to secure (amongst other aims) IOP for all market participants:

- In 1990, the European Commission published the so-called Open Network Provision (ONP) Directive (90/387/EEC). This directive mentions the possibility of defining harmonised conditions for technical interfaces. It further specified the role of ETSI in the creation of European standards and it specified that European standards should be made mandatory where this is strictly necessary to ensure the IOP of cross-border services and to improve freedom of choice for users.
- In 1992 and 1993 Directives 92/44/EEC and COM 93/182, which further specified the application of the original ONP Directive. Both directives stipulated that applied standards and technical interfaces be published by network operators to promote harmonisation and interoperability of services.
- In 1996, the European Parliament and the Council published a Directive on Interconnection in Telecommunications with regard to ensuring universal service and interoperability through application of the principles of Open Network Provision (COM (96) 535 final). Its objectives included promoting the development of trans-European networks and the interoperability of national networks.
- In 1997, the Directive on Interconnection in Telecommunications with regard to ensuring universal service and interoperability through application of the principles of Open Network Provision (97/33/EC), proposing a harmonised framework for interconnection of public telecommunications networks in Europe. In this context, NRAs could set conditions for interconnection agreements to ensure interoperability of telecommunication services.
- In 2002, the European Commission published the regulatory framework currently still in force, which obliges NRAs in Europe to ensure IOP for telecommunications networks.

40 Wikipedia and The History And Future Of Message Interoperability

At a technical level, the European Standards Organisation ETSI supported interoperability efforts inter alia by adopting SS7, which is used for call routing, for mobile networks and later the GSM standard for mobile networks, the first common standard in Europe for wireless networks, which later became a worldwide standard. Later released standards by ETSI are for example on Voice over IP (VoiP) and Voice over LTE (VoLTE).

However, standard organisations like ETSI, ITU and later 3GPP had to agree upon these standards by determining the lowest common denominator for standardisation. The consequence was that many countries specified their own national extensions of standards, which led to higher costs as each country had a different implementation and/or equipment vendors needed to comply with different set of standards. Furthermore, the interconnection of networks between different countries was complicated by this. Another consequence of pursuing interoperability is that the functional services offered over fixed and mobile networks over the years have not changed or expanded much in functionality as this would require expanding the standards to ensure interoperability for the new functions.

Interoperability for SMS and MMS

The first short SMS was sent from a PC to a mobile device in 1992 by Vodafone in the United Kingdom. However, it took in Europe until April 1999 for interoperability for SMS being implemented between mobile operators and until 2002 before it was implemented in the USA.[41] Only from this moment onwards customers could really start using the service to ‘text’ all of their contacts across the different telecom networks. Within a year, SMS traffic grew dramatically and exceeded 400 million messages per month.[42] In the US, standards organisation CTIA started discussing text messaging standards in October 2001 and started working groups to identify a common feature set, which eventually led to a first standard around 2009.[43]

The successor of SMS, called Multimedia Messaging Service (MMS), promised customers to exchange more than just 160 characters. Unlike SMS, MMS can deliver a variety of media, including up to forty seconds of video, one image, a slideshow of multiple images, or audio between mobile phones but also PCs and Personal Digital Assistants devices.

The first mobile operators started with picture messaging around 2000. However, there were different technology standards and media formats used in mobile networks and the internet; GSM operators wanted to use the traditional E.164 phone address where the

41 Crowe, David 2002. "SMS Interoperability: Canada Leads the Way." http://cnp-wireless.com/ArticleArchive/WirelessTelecom/2002Q3-SMSInterworking.htm

42 CDMA development group paper, March 2004, “MMS Inter-carrier & Inter-standard Interoperability. An industry solution”. See http://www.cdg.org/technology/applications/files/mms_paper.pdf

43 CTIA (2013), SMS Interoperability Guidelines, Version 3.2, Effective Date: February 5, 2013.

PC industry looked at the IP based addresses.[44] In October 2002, the mobile industry started a global organisation called the Open Mobile Alliance (OMA) to focus on establishing interoperability and open standards. Around 2003, the first MMS specifications where observed, but not all global standards bodies supported the same media formats and the MMS standards did not define how these different media formats should be transcoded when messages are sent between different networks (e.g., CDMA, GSM and IP-based services). In March 2004, interoperability testing was still ongoing in the OMA [45] and only in January 2006, the Internet Engineering Task Force (IETF) communicated a proposed standard (Request for Comments – RFC 4356) to exchange messenges between multimedia messaging services and internet mail systems.[46]

In conclusion, we note that the functionality of SMS and MMS has not changed over time, which maintained interoperability, but limited innovation although use cases have evolved to include application to person communications.[47]

RCS

Rich Communication Services (RCS) aimed to replace SMS and MMS messenges with a text-message system that is richer, provides phonebook polling (for service discovery), and can transmit in-call multimedia.[48] The process started as an industry initiative in 2007, and became a formal GSMA project when the GSMA established an RCS steering committee in 2008. In December 2008, the first version of definitions (and hence interoperability between participating operators) was released for enhanced voice calling and enhanced chat, which was subsequently expanded with more functions until 2011 with the specification for RCS-e (enhanced). From 2012 onwards, the first commercial launches with the name ‘Joyn’ were seen in the market (Spain, US, South Korea, Germany). Thus, it took around 4 years from standard development until first commercial launches with operators offering an interoperable service.

The RCS-e standard then evolved in the RCS Universal profile of the GSMA of which the first version launched in November 2016. From this time on, commercial launches under the name RCS, Universal Profile or Message+ are observed in the market (US, Canada, Norway, Hungary). As recently as April 2020, in Switzerland Message+ was introduced.[49]

44 So called ENUM servers tried to resolve the translation between E.164 phone numbers and internet URI like mrsmit@hotmail.com for the routing of MMS between mobile networks and internet servers. Home network HLR queries are used by mobile operators to route MMS messages and via a so called MAP query, the MMS routing information is retrieved.

45 See http://www.cdg.org/news/events/cdmaseminar/2003_Tech_Forum/Qualcomm.pdf

46 See https://datatracker.ietf.org/doc/rfc4356/

47 The significant development is the usage of the service over time; where it started as a person to person service, there has been an shift to application to person facilitated by providers (like twilio.com or gatewayapi.com), who provide APIs to connect their SMS gateway to a customer’s application.

48 Wikipedia, see https://en.wikipedia.org/wiki/Rich_Communication_Services. RCS functionalities cover among others: Standalone Messaging, 1-2-1 Chat, Group Chat, File Transfer, Content Sharing, Social Presence Information, IP Voice call (IR92 and IR.58), IP Video call (IR.94) and Geolocation Exchange.

49 See https://community.swisscom.ch/t5/Telephony-Knowledge-Base/RCS-introducing-the-future-of-SMS-Message/ta-p/612475

It is noted that these functions overlap significantly with the functions that have been offered by OTT service providers over a significantly longer period for no monetary fee. As the gradual establishment of standards for these functions have shown, it takes time to agree upon standards for more complicated functions and for them to be introduced in the market. Moreover, as consumers have shown themselves to be satisfied with the faster evolving (non-interoperable) OTT services, and are willing and able to multihome[50], it is unclear whether RCS will gain traction in the market. According to market research, the RCS market is expected to grow from 2.3 billion USD in 2020 to 4.8 billion USD in 2026 with an annual growth rate of more than 14%.[51] However, it remains limited in scale compared with other telecom services.

Number portability

In addition to offering interoperability for basic telephone services, the telecom sector providers an example of data portability in the form of (mobile and fixed) number portability. Existing customers of telecommunication services are allocated a unique telephone number, which is allocated to a number pool of a certain provider. In this manner, all operators over the world know to which network voice calls and SMS messages should be routed when addressed to this phone number. When changing provider, this number can be ‘ported’ to the new provider, so that the customer can retain his phone number ID and can still be reached by all of his contacts. This represents one-time asymmetric data porting and has been mandated by regulation from the 1990s onwards to promote competition when alternative fixed and mobile operators entered the market following the liberalisation of the sector. The European Commission Directive 98/61/EC required that mobile number portability should be available to consumers in January 2000.

Although regulators set deadlines for the introduction of number portability, the technical implementation and required coordination process was left to the industry and differs per country. In general, a so called ‘recipient-led’ systems was implemented, which means that the customer wishing to port its number requests this from the new network operator (recipient), which then contacts the current network (donor). However, there are exceptions with UK and India using a ‘donor-led’ system. There are also different technical solutions with regard to the routing of voice calls, SMS and MMS after porting, which were left to the discretion of each country. Most countries used a central database of ported numbers, which is then used by all operator to find out where to route their calls. This is known as the All-Call-Query/Central Database solution. However, the resulting porting time was very different and varied from a couple of seconds (New Zealand) and a couple of hours (Ireland) to as much as 5 days in the UK.

---

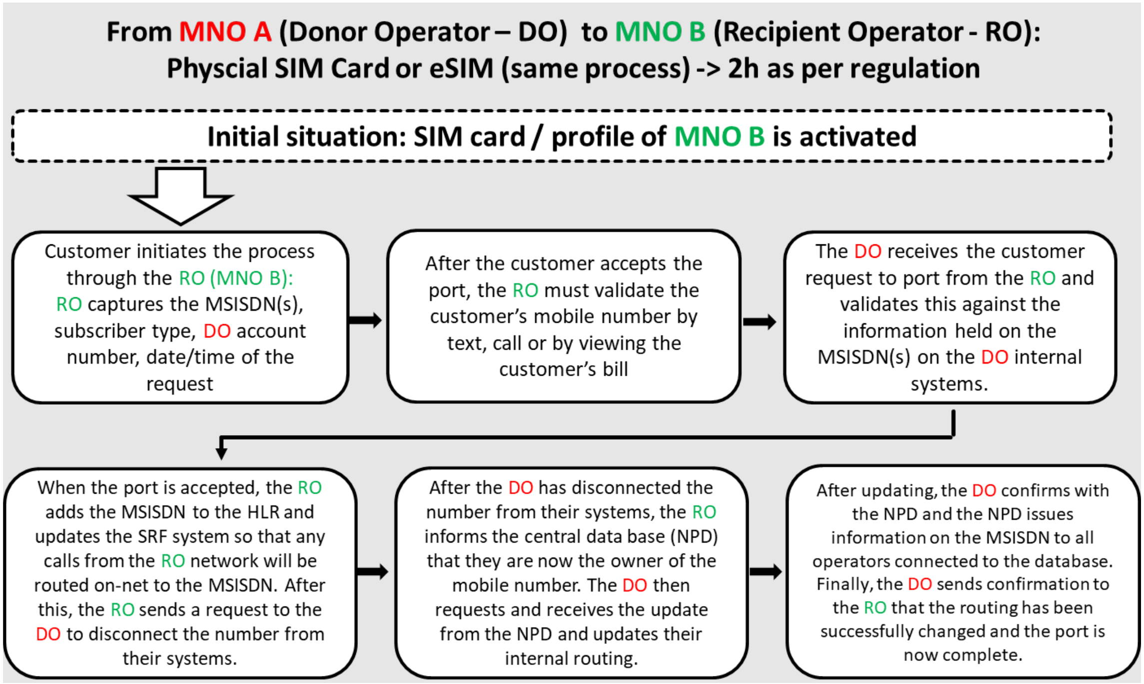
50 WIK‘s Study on multi-homing in 2021 shows that 91% of interviewed consumers use internet based communication services and that 95% of these apply multi-homing and use on average 5,4 different OTT (communication) services. See Kommunikationsverhalten (wik.org)

51 See Rich Communication Services (RCS) Market | Size, Share, Growth | 2022 to 2027 (marketdataforecast.com)

It is interesting to note that in Europe, despite setting a deadline for its introduction of 2000, the implementation of MNP took considerably longer, with most countries implementing MNP between 2002 and 2006, but with some countries which were as late as 2014.[52]

An example of the MNP process developed over time in Ireland is shown below.

Figure 14 Mobile number portability Process in Ireland



Source: WIK-Consult based on Mobile Number Portability Process Manual Issue 6.01, p. 19f.

The porting of the number in the context of electronic communications is associated with switching, because it is no longer possible to use the previous service provider for voice calls or SMS once the number porting has been completed. Thus, the process also involves the termination of the old contract. This is carried out by the Recipient Operator, which contacts the Donor Operator to terminate the contract and perform number portability at the request of the end-user. It is interesting to note in that context that obligations regarding number portability fall both on the donor and the recipient operator in order to ensure a smooth process for customer migration.

52 See https://en.wikipedia.org/wiki/Mobile_number_portability

4.3.2 Banking

The banking sector has been subject to efforts to support interoperability and portability to enable digital transactions between banks (horizontal interoperability), facilitate entry and competition in banking services (vertical interoperability), and to facilitate switching by consumers from one bank account to another (data portability).

Similar to the telecommunications sector, standards for interoperability took several years to develop and implement and data portability is linked to switching i.e. the closure of one account alongside its replacement with another, with the aim of ensuring that the customer maintains his transaction records and instructions after switching providers.

Inter-bank transaction interoperability

Early efforts to achieve interoperability in the banking sector can be traced back to the development of the Home Banking Computer Interface (HBCI) in Germany. This open standard for customer self-service machines and electronic banking took 4 years to create and was officially launched in 1998.[53] Key elements of the standard included security protocols, message formats and transmission procedures. The system was replaced by Financial Transaction Services in 2002, which provided a procedure for Personal Identification Number (PIN) codes to access accounts coupled with a single-use transaction authentication number (TAN). In 2003, an ISO standard was adopted for financial transaction card originated messages.[54] The standard was designed as an interface specification allowing messages to be exchanged between different commercially designed applications.

Market opening mechanisms

Efforts to open up the banking market to new entrants followed in 2007, with the introduction of the first EU Payment Services Directive.[55] This instrument created a new category of payment service providers and a regulatory framework which explicitly permitted non-banks to execute financial transactions.

The second Payment Services Directive (PSD2), adopted in 2018 built on its predecessor to further open payment services to competition, by mandating access to certain forms of data. Under the measure, payment service providers are required to provide access to specific functionalities such as account balance enquiries, and identification. Two types of official payment service providers are identified under the PSD2: Account Information Service providers, which are authorised to access account data and payment systems with consumer consent, and Payment Initiation Service Providers, which can access data as well as initiating payments.

---

53 https://nordigen.com/en/blog/origins-open-banking-brief-history-industry-altering-tech/
54 https://www.iso.org/obp/ui/#iso:std:iso:8583:-1:ed-1:v1:en
55 https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32007L0064

The UK has been at the forefront of developments in open banking, supporting the development of an Open Banking Standard via a common API. The intention was to establish a standard, whereby individual services in the banking and financing sector could be disaggregated and offered on a modular basis with the aim of reducing lock-in effects and switching costs as well as introducing a platform on which customers could freely choose from the offers of multiple providers. (Open Banking, 2022a) For the second quarter of 2021, Open Banking reported 319 third-party providers as participants in the Open Banking ecosystem with over 800 million API calls per month. (Open Banking, 2022b) [56]

APIs enable payment service providers to connect to users' bank accounts and access account information, such as:[57]

- **Account:** account holder name, a list of account holder's accounts (account number, IBAN)
- **Transactions:** date, merchant or counterparty (partner) name, description (info field), amount
- **Balances:** current and available

Banking intermediaries can then analyse this data to provide value added services such as the categorisation of transaction data, and analysis of patterns which could highlight irregularities and help to identify fraud as well as understanding customer behaviour and requirements. Access to banking data from multiple sources could also enable service providers to develop applications which allow consumers to view different bank accounts in one place.[58]

Portability

The Payment Account Directive (2014)[59] also encourages the use of standardised processes to enabling consumers to switch from one bank to the other, including the sharing of historical transaction records and porting of payment instructions.

The receiving payment service provider initiates the switch at the request of the consumer, and within 2 days of receiving their approval, requests information from the transferring payment provider (the donor) about existing standing orders, credit transfers and direct debits, transfers the remaining positive balance and closes the previous payment account.[60]

---

56 Open Banking. (2022a). About the Open Banking Implementation Entitiy. Retrieved from https://www.openbanking.org.uk/about-us/ Open Banking. (2022b). FINTECHS. *Open Banking*. Retrieved from https://www.openbanking.org.uk/fintechs/

57 https://nordigen.com/en/account_information_documenation/api-documention/overview/

58 https://www.thalesgroup.com/en/markets/digital-identity-and-security/banking-payment/digital-banking/psd2/open-banking

59 https://eur-lex.europa.eu/legal-content/GA/ALL/?uri=celex:32014L0092

60 See article 10, the switching service.

The new payment service provider must then set up standing orders and direct debits within 5 days of receiving information from the donor provider.

4.3.3 Interoperability in email and USENET newsgroups

It should be noted that certain Internet services are also interoperable, including email[61] and USENET newsgroups.[62] However, these were developed from the outset with the aim of providing interoperable platforms for communication. Email continues to be widely used, and is indispensable for the vast majority of Internet users, including businesses. However, it is interesting to note that innovation in email has been relatively limited, as innovation has evolved primarily through a host of proprietary messaging systems. Meanwhile, Usenet is still available, from a technical perspective. However, its use is limited, as a wide range of social media applications overtook and significantly elaborated on its potential to enable different users to post information and share views.

4.3.4 OTT messaging services

The subject of interoperability in messaging services has received considerable attention in recent years, in particular with the inclusion in the Digital Markets Act of a provision that platforms which are designated as “gatekeepers” should make available end-to-end text messaging including various kinds of media attachments, interoperable on request by a competing service.[63] Although the obligation extends in the first instance only to

---

61 In 1982, the Simple Mail Transfer Protocol (SMTP) was released by the University of Southern California and ARPAnet released in the same year the standard for ARPA Internet text Messages (RFC 822, 13 August 1982, https://datatracker.ietf.org/doc/html/rfc822 and RFC 821, https://datatracker.ietf.org/doc/html/rfc821). The SMTP protocol enables the transmission of an electronic mail from someone’s computer and between mail hosts in the Internet. IETF released in 2008 the following related standards RFC 5321 and 5322, and extensions in 2012 with RFC 6531. In 1988, the first versions from the Internet Message Access Protocol (IMAP) were designed and released. IMAP is an Internet standard protocol used by email clients to retrieve email messages from a mail server over a TCP/IP connection. It was developed beside the already existing Post Office Protocol (POP) to have more control over your mailbox. Virtually all modern e-mail clients and servers support IMAP, which along with the earlier POP3 (Post Office Protocol) are the two most prevalent standard protocols for email retrieval. In 2012, ETSI updated the standards for e Mail to enable internationalized email with RFC 6530. The IETF started a technical and standards working group devoted to discussing issues of email addresses at international level.

62 In parallel to eMail and the internet, a separate worldwide electronic network, called Usenet, came to life in 1979 at the University of North Carolina at Chapel Hill and Duke University. Usenet, short for Unix user network, is a set of protocols for generating, storing and retrieving news "articles" (which resemble Internet mail messages) and for exchanging them among a readership which is potentially widely distributed. These so called newsgroups, are free for everyone to participate. In June 1983, the first formal specification of the messenges exchanged by UseNet, was released RFC 850, https://datatracker.ietf.org/doc/html/rfc850. It was superseded by RFC 1036 and subsequently by RFC 5536 and RFC 5537

63 Article 6 DMA. The provisions extend well beyond provisions included in the EU Electronic Communications Code which did not establish an interoperability requirement, but rather empowered NRAs to oblige (proportionate) interoperability for interpersonal communication services (ICS, including number independent ICS) where the end-to-end connectivity is endangered due to a lack of interoperability. These ICS should have reached a significant level of coverage and user uptake, and the threat to end user connectivity should been confirmed in a consultation with BEREC.

"basic functionalities", it is envisaged that group chats and end-to-end voice and video calls will also be captured within 4 years following a gatekeeper designation.

This interest revives a debate that began in the early part of the 21st century, when the US FCC imposed conditions on AOL, which at that time operated the leading instant messaging (IM) service, at the time of its merger with Time Warner. Specifically, the FCC restricted the merged company from offering advanced IM services such as videoconferencing until it either implemented an industry-wide standard or enabled interoperability standards between its IM system and that of three other competitors.[64] In 2003, AOL submitted a petition for relief from the Instant Messaging Interoperability requirements,[65] a request which was granted by the FCC in August 2003.[66]

From subsequent developments, it is notable that AOL did not maintain its leadership in Instant Messaging, and that many other video-conferencing solutions emerged, highlighting the dynamic nature of competition in the sector. The development of alternatives and multi-homing practices of consumers[67] suggest that an interoperability obligation was indeed not essential in enabling consumers to be able to benefit from competition in this area and may have held back the regulated firm from engaging in this innovation.

Moreover, the fact that video-conferencing interoperability took many years to be addressed in the context of RCS (despite the apparent interest of mobile operators in providing a competing solution to OTT NIICS), tends to confirm that mandating interoperability on video-conferencing was not a straightforward remedy, raising questions about whether the benefits of an obligation (in the absence of the threshold conditions identified to justify NIICS interoperability requirements in the EU Electronic Communications Code) outweigh the costs. [68]

4.4 Overview and lessons

Interoperability and portability obligations have been successfully introduced, most notably in telecoms and banking, while basic online services such as email (and USENET) were designed to be interoperable from the outset. However, it is notable that in all cases, interoperability has been service-specific and focused on basic functions such as calls, email and details which are essential for inter-bank communications while

64 http://www.fcc.gov/Bureaus/Cable/Public_Notices/2001/fcc01011_fact.pdf
65 https://docs.fcc.gov/public/attachments/DA-03-1092A1.pdf
66 http://www.techlawjournal.com/topstories/2003/20030820.asp
67 See WIK's Study on multi-homing in 2021 shows that 91% of interviewed consumers in Germany use internet based communication services and that 95% of these apply multi-homing and use on average 5,4 different OTT (communication) services. See Kommunikationsverhalten (wik.org).
68 Art 61 b) and c) of the EECC empower NRAs to oblige (proportionate) interoperability for interpersonal communication services (ICS, including number independent ICS) where the end-to-end connectivity is endangered due to a lack of interoperability. These ICS should have reached a significant level of coverage and user uptake, and the threat to end user connectivity should be confirmed in a consultation involving BEREC.

portability has focused on specific key data points. Even with this limited scope, experience shows that introducing standards and consequent implementation of interoperability involved considerable time (multiple years) and effort on the part of the industry.

Where there has been horizontal interoperability (such as in voice, SMS, eMail interconnection), there has been limited subsequent innovation in the service concerned – although innovation has flourished in the surrounding unregulated environment (as can be seen for example in the case of OTT NIICS services). New standards which reflect those innovations have tended to be introduced only once those innovations have been embraced by consumers in the wider market, following a significant period, as can be seen for example in the case of RCS and video calling.

Data portability has played a crucial role in facilitating switching both in the telecoms and banking sectors. However, it is important to note that in both these sectors, consumers are likely to rely on a single main provider, in stark contrast to online behaviour, where consumers and business customers often (although not always)[69] multi-home. Portability in these cases is based on the transfer of a clear set of data which is essential for identification and for the performance of the service (such as a telephone number, account number, data regarding standing orders), which can be easily interpreted by a rival provider. Moreover, it is interesting to note that in both cases, responsibility for ensuring portability and subsequent switching lies with both the donor and recipient.

The provisions on “Open banking” provide an interesting example showing how vertical interoperability can facilitate downstream competition and innovation in the use of data and provision of user-friendly interfaces for consumers. However, this example is focused on facilitating access to basic identity and well-established transactional data in the specific case of banking with a view to stimulating innovation on “over-the-top” services in a sector which was otherwise largely mature and was not characterised by significant innovation by the major financial institutions.

69 Multi-homing is prevalent in the case of NIICS. Surveys also show that business customers favour multi-cloud solutions.

Table 1 Overview of interoperability and portability in different sectors

Sector / service	Relevant legislation / date	Standards / date	Aims	Scope of interoperability	Scope of portability
Telephony, including calls, SMS and RRC	ONP Directives	SS7 for fixed- and mobile networks / 1975	Standardised call routing on fixed and mobile networks	Voice call routing	None
	EU Framework for Electronic Communications	GSM / 1987	Standard for mobile communications	Mobile calls and data messages	None
	EU Directive 98/61/EC (MNP) / 1998	Implementation differs per country, from 2001 onwards	Having a NP solution implemented by 2000 which was supported by national operators.	Voice call and data message routing for fixed and mobile networks	Fixed and mobile phone Number
	EU Electronic Communications Code	VoIP / 2004 (ETSI TR 101 301 V3.1.1 (2004-04))	Voice over IP	Voice calls over fixed and mobile IP networks	None
		VoLTE (ETSI TS 103 397 V1.1.2 (2020-03)	Voice over LTE	Voice calls over mobile LTE networks	None
		SMS (ETSI ES 202 060-3 V1.1.1 – 2003)	Exchange of SMS across networks	SMS only	None
		MMS (ETSI TS 122 140 V5.3.0 (2002-09)	Exchange of MMS across mobile networks	MMS only	None
		RCS / 2008-2016 (ETSI TS 102 901 V5.1.1 (2013-10)	Exchange of RCS across mobile networks	RCS only	None
Email	Internet Engineering Task Force (IETF)	1980, with updates in 2008 and 2013	Setting standards for using addresses, message syntax	E-Mail only	
Banking		ISO standard for financial transaction card originated messages ISO 8583-1:2003	Interface for the exchange of messages between different applications	Horizontal interoperability for financial transaction card originated messages	
	PSD1 2007		Create category of payment service providers, permit non-banks to execute financial transactions		

Sector / service	Relevant legislation / date	Standards / date	Aims	Scope of interoperability	Scope of portability
	Payment Services Directive (PSD2) 2015, entry into force 2016, applied from January 2018		Open payment market to new entrants Establish single euro payments area	Vertical interoperability, which could be facilitated via banking-specific APIs covering account details, transactions and balances	
	Payment Accounts Directive (2014)		Encourage standardised processes to enable consumers to switch between banks		Data regarding transactions, process for account closure and balance transfer

5 What does interoperability and portability potentially mean in the cloud and how can these concepts apply in practice?

In this chapter, we provide an overview of what interoperability and portability mean in a cloud context, with reference to ISO standards. We then run through different scenarios that may be relevant to cloud enterprise customers and consumers, and discuss how interoperability and switching is achieved in practice, and who is responsible for which aspects. Key conclusions are:

- **Cloud interoperability** can be defined with reference to the ISO "5 facet" model, which distinguishes different levels of interoperability from transport of data through to mutual recognition of data formats, interpretation of the data and finally the ability of two systems to deliver expected results. Compatibility in legal norms is also considered.
- **Cloud portability** can involve porting (virtual) "infrastructure" from on-premises data centres to the cloud or between different clouds, through to the porting of platforms, applications and data. Portability of applications can be described with reference inter alia to whether instructions execute on the new platform and whether the outcomes are as expected. Data portability can be described with reference to whether the data is received in a readable structured format and whether the ported data can be understood. Mutual compliance with relevant laws can also affect the degree to which portability can be achieved.
- Switching (in terms of the replacement of one service with another equivalent service) is often not relevant for the cloud because services differ in functionality. However, **migration** is relevant, and can be understood as portability of the relevant infrastructure, application or customer data potentially in conjunction with the termination of the contract, and the initiation of the integration with other systems in a way that allows business continuity.
- From a business customers' perspective, the customer journey might involve the following steps: (a) migrating from an on-premises solution to the cloud or adding additional cloud native applications; (b) linking the remaining on-premise servers or applications with the cloud (hybrid cloud); (c) making use of services from different cloud providers (multi-cloud); (d) building on cloud platforms or applications to add further functionality; and (e) switching from one cloud service provider to another. Migrating and switching involve portability of data and applications, while hybrid and multi-cloud solutions require a degree of horizontal interoperability. Building on existing services can be viewed as a form of vertical interoperability.
- Many businesses have yet to take the first step in this journey (migrating to cloud). The process of migrating some or all of a businesses' IT functions from on-premises data centres to the cloud is complex and requires the customer to make decisions

about which functions to entrust to the cloud and how to ensure that its applications continue to interoperate in the new environment. Different options are available ranging from “lift and shift”, through to “refactoring” and “replacement”.

- The process of IT **migration in general for an enterprise is project-based** and can take several months or more depending on the scale of the enterprise and the number of integrations with other products and entities. There is limited practical experience so far of major switches for enterprise customers between different cloud providers, but the complexity, time and cost are likely to depend on customer choices about which services to procure from the cloud, the complexity of applications and the size of databases and data that they plan to move. Tools provided by cloud service providers may help to streamline the process in some cases, but it is inevitable due to the diversity of the choices for the customer and products involved that this process too will be project-based.
- Enterprise customers are increasingly linking their on-premises and cloud capabilities and making use of multi-cloud solutions. These can include for example for IaaS being able to make use of back-up computing capacity, or for PaaS the availability of a back-up database. These **common use-cases require a degree of interoperability**. This is **well-established at the IaaS layer** e.g. where two cloud services have a common understanding of data models such as virtual machines and containers, while at the **PaaS layer, customers may opt to choose similar databases** (on different providers) to ensure similarity in data format and structure. **SaaS applications are very diverse**, but there may be a need to exchange data between applications. If the data does not have the same structure and semantics, **data transformation may be an option, but is done on a case-by-case basis**.
- Leveraging existing cloud services to provide add-on services is an important opportunity for both enterprise customers and application developers. Many cloud-native applications are built on software architectures and standards like REST, XML and Json to facilitate this possibility – which is an example of vertical interoperability. The cloud service receiving data input should have a well-defined API that the first cloud service can use. There have been efforts to develop **APIs for downstream application development in specific sectors which involve common datasets and goals** such as banking and healthcare.
- Data portability and switching may also be relevant for consumers, who make use of “SaaS” services such as content lockers, cloud-based productivity software or back-up. In addition to consumers’ right to download their personal data, consumer SaaS switching can be facilitated by using **standardised file formats** e.g. for video-encoding or through conversion tools. However, **equivalence of functionality cannot be achieved** without undermining the potential for different applications to differentiate their services.

5.1 What does cloud interoperability and portability mean?

Cloud interoperability

Cloud interoperability is defined (ISO/IEC 2017) as the ability of a Cloud Service Customer (CSC)'s on premises system to interact with a cloud service or the ability for one cloud service to interact with other cloud services by exchanging information according to a prescribed method to obtain predictable results.[70]

ISO (2017) defines 5 aspects (or "facets") of cloud IOP: transport, syntactic, semantic data, behavioural and policy.

Transport IOP relates to the communication infrastructure between cloud computing components like HTTP/S and Advanced Message Queuing Protocol. Syntactic IOP is the ability of these systems to understand the structure of exchanged information via encoding like JSON and XML and semantic data IOP requires a common understanding of the data models used such as virtual machines at infrastructure level, the deployment environment at platform level and at application level, concepts of the application itself including customer specific concepts such as the 'patient' in healthcare applications or 'customer' in an order entry application.

Behavioural interoperability is when two cloud services exchange information via an interface (API) and the result is coherent with the customer expectations. This is mostly defined in the service description including the interface, the set of operations provided and the in- and outputs of each operation and the conditions required to fulfil the operations properly.

Policy interoperability is where these two cloud systems interacting with one another also comply with the legal, organizational and policy frameworks. Examples are regulations regarding sensitive data like personal, health, financial and governmental data. Examples of the different facets are shown in the following table.

70 ISO/IEC 19941:2017 (E), Information technology – Cloud computing – Interoperability and portability.

Table 2 The different aspects (facets) of interoperability – ISO 2017

Facet	Aim	Objects	Solutions
Transport	Data transfer	Signals	Protocols of data transfer, e.g., REST over HTTP; MQTT
Syntactic	Understand format of transferred data	Data	Standardized data exchange formats, e.g., XML
Semantic data	Interpretation of transferred data using a data model	Information	Common data models, e.g., OData, OWL
Behavioral	Get anticipated outcomes when making service requests	Programmatic interface	UML models, pre-conditions, post-conditions, constraint specifications
Policy	Ensure that interacting systems conform to applicable laws, regulations and organizational policies	Laws, regulations, policies	Conditions for operation

The applicable service model for cloud services (IaaS, PaaS, SaaS), determines whether the responsibility for these facets of interoperability lies with the cloud service provider (CSP) and/or the cloud service customer (CSC):

- For IaaS, the CSP takes care of the transport and syntactic aspects of the data. All other aspects are still the responsibility of the CSC.
- In case of PaaS, in addition to the required infrastructure the CSP also manages the development tools, including the semantic aspect of using a specific data model. The CSC is however still responsible for the functioning of the developed application and hence responsible for the outcome of the functions (the behavioural aspect) and compliance with regulations and other policies.

When conceptually relating these facets to the concepts of horizontal and vertical interoperability, the following considerations apply:

- Horizontal interoperability, referring to interoperability between comparable services (hence competing with one another), would use a common standardized transport infrastructure, so the focus for establishing interoperability would be on all other aspects. This would start with the syntactic and semantic aspects to ensure that exchanged data is understood in both cloud services. Thereafter, the behavioural aspect relating to the proper functioning of the applications hosted in the cloud once interoperable with applications in other clouds and/or on-premises. And finally on the policy aspect to see whether the whole setup still complies with applicable regulations and policies.

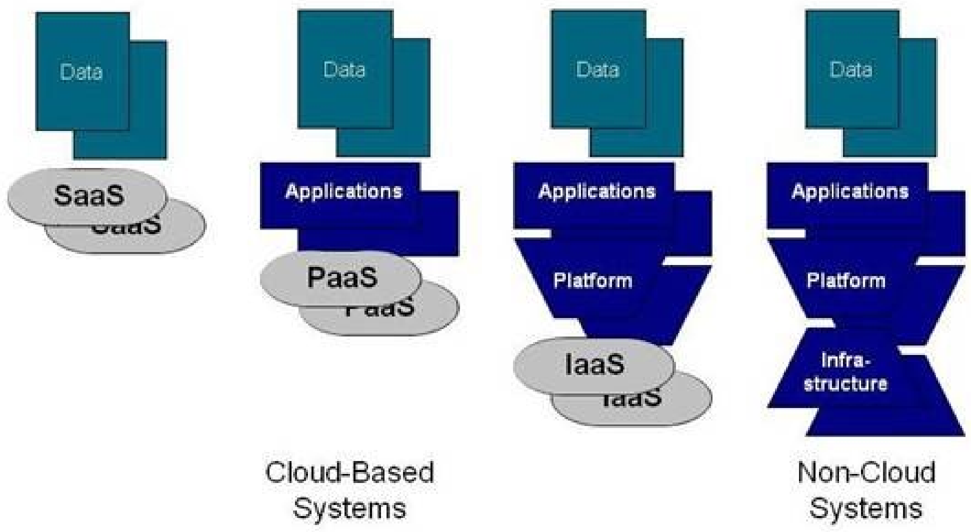
- Vertical interoperability, referring to the 'bolting on' of specific functions down or upstream to an application (e.g. payment function to an e-Commerce platform), could have a more limited scope. In the case of asymmetric vertical interoperability, whereby, the added function is just extracting information from the main application, the syntactic and semantic aspect would be the focus to ensure the proper functioning of the added function. With symmetrical vertical interoperability, there is still an exchange of data, although it is likely that less functions are involved compared with horizontal IOP, but still all aspects (apart from transport) would need to be addressed.

Cloud portability and switching

Cloud data portability is defined as data portability from one cloud service to another cloud service or between a CSC's system and a cloud service.

Depending on the level of the value chain where porting occurs, the concept of portability in the context of cloud computing could in theory involve the porting of platforms, applications, documents and data, as shown in the following diagram.

Figure 15 Portability concept for Cloud computing



Source: OpenGroup[71]

The Cloud Standards Customer Council further elaborates on the meaning of "cloud data portability" distinguishing between Syntactic, semantic and policy facets of data portability, as shown below in the first table. It has also defined the portability of applications through a 5-facet model (second table below).

71 http://www.opengroup.org/cloud/cloud_iop/p4.htm

Table 3 The different aspects (facets) of data portability – CSCC

Facet	Aim	Objects	Examples
Syntactic	Receive data in a readable structured format	Data	JSON, XML
Semantic	Understand the meaning of ported data	Information	OWL
Policy	Meet applicable laws, regulations and policies	Laws, regulations, policies	Personal data regulations, Cross border data transfer laws, Security policies

Table 4 The different aspects (facets) of application portability – CSCC

Facet	Aim	Objects	Examples
Instruction	Execute application instructions correctly	Executable artifacts	Java, C++, BPEL
Syntactic	Understand and use format of application artifacts	All application artifacts	Zip, tar, jar
Metadata	Understand and use the metadata that specifies environmental dependencies for executing the application	Metadata artifacts	YAML, JSON, Script, XML
Behaviour	Produce the expected results when executing the application	Application functional and non-functional behaviours	Verified by test suites
Policy	Meet applicable laws, regulations and policies relating to application use	Laws, regulations, policies	Personal data regulations, Cross border data transfer laws, Security policies

Switchability is not a term that is commonly used in relation to cloud services, because services are diverse and are not typically fully equivalent. However, ease of migration is relevant and could refer to the ease with which, potentially alongside portability (where relevant), end-users can terminate a contract with one provider in order to procure similar services from another provider.

5.2 In what situations might cloud interoperability and/or portability potentially apply and how does it work?

Drawing on the ISO 2017 standards document alongside a Guide from the Cloud Standards Customer Council[72], we have identified a number of scenarios where cloud interoperability and/or portability might be relevant. We have put those in logical order from the (enterprise) customer perspective.

72 Cloud Standards Customer Council (2017), Interoperability and portability for Cloud computing: A Guide.

1. Migration of customer capabilities from on-premises services into cloud services and/or adding cloud-native applications[73],[74]
2. Customer links in-house capabilities with cloud services
3. Customer uses cloud services from multiple providers
4. Customer (or application provider) links one cloud service to another cloud service
5. Customer migrates between CSPs

The previous scenarios assume that the customer is a business end-user. However, migration, switching and multi-cloud use are also relevant (for SaaS) for consumers. We therefore consider also the following consumer scenarios:

6. Consumer uses multiple "cloud" services, but then wishes to move some data from cloud provider A to B and then completely migrate from provider A to B
7. Consumer uses multi cloud services and wants to share data between the applications.

In each of the scenarios we highlight possible applications of interoperability and/or portability at the different levels of the value chain and in this context, we make reference to the terms IaaS, PaaS and SaaS, drawing on the classifications described in section 3.1. However, we note that over time, the boundaries between these categories have become increasingly blurred (in particular between IaaS and PaaS), and this should be taken into account when seeking to define boundaries from a legal or regulatory perspective.

Important points to note from these scenarios are that the processes involved are specific to different situations and the complexity depends on choices made by the customer.

5.2.1 Customer migration to cloud (scenario 1)

As the cloud is a rather recent development in the market and a significant proportion of businesses (in particular SMEs) have not yet taken advantage of cloud computing, the first step that an enterprise customer may consider is moving the capabilities provided by certain in-house servers, applications and services to cloud service solutions to save costs, be more agile etc.

---

73 This are discrete, reusable components known as microservices that are designed to integrate into any cloud environment. These microservices act as building blocks and are often packaged in containers. See www.ibm.com/cloud/learn/cloud-native

74 Instead of migrating customers might start using so called cloud-native applications. As cloud computing provides new ways to build applications and run them (e.g. virtualisation, containerisation), there are many new applications available in the cloud which did not exist on-premise or in any hybrid cloud context. In this case there is no migration (scenario 1), but all other scenarios such as the integration of these additional applications with other applications may still apply.

The process of migrating from on-premises to the cloud requires a number of decisions from the customer, including which aspects of their in-house IT solution to migrate to or replace with a cloud solution, and which aspects of the infrastructure, platform and service provision to entrust to the cloud provider. Therefore, this process is generally project-based. This applies to all of the sub scenarios below.

- Migrating virtualized premises applications to an IaaS service tend to be the lowest effort, since the complete software stack is migrated by packaging it as one or more virtual machines, which are imported in the cloud service and executed. This scenario is often described as "***lift and shift***", and should in theory provide the environment that is closest to that which was provided in-house. However, the customer needs to bear in mind that the original application was built in a local area network with low latency, and thus needs to consider whether the migrated application can cope with the higher latencies associated with cloud service environments. Furthermore, this scenario assumes that the application is licenced and supported by the application developer to run in the cloud environment.
- If the customer migrates from on-premise applications to a PaaS solution, it is likely that they will need to rewrite their on-premise applications, a process known as "***refactoring***", as the full PaaS infrastructure that is available in the cloud, is not typically available in an on-premise environment.[75] Thus, customers tend to undertake this migration when their existing application needs a significant upgrade or another significant change is due (such as licence renewal).Before taking this step, the customer needs to consider the required effort to rewrite the application in the new PaaS environment. Furthermore, the customer needs to examine if the historic data can be loaded into the PaaS cloud service.
- An application often has linkages via APIs to other applications. When migrating to PaaS/IaaS cloud services and/or adding cloud-native applications, the (continued) interoperability of the migrated and/or new customer application with other applications depends on (a) the sophistication of the customer's existing environment to provide great modularity between functions and (b) the facilities available from the cloud service provider. Furthermore, in this scenario, any differences in the performance of the migrated application need to be considered and the resulting impact on other applications connected via APIs. For example, customers need to consider the bandwidth and latency of the connection between their data centre and the CSP. Normally the bottleneck is at the customer's end as the connection speed of typical hyperscale CPS data centres to the Internet is around 10x to 10,000 times faster than the connection at the customer's data centre.

---

75 For example, MS Azure can be considered as a kind of Lego toolkit with 200 different building blocks.

- If the customer procures a SaaS cloud service, he moves from using an on-premises application to a SaaS cloud service. This is effectively a "***replacement***" of the on-premises solution, and the application code does not need to be ported. However, it may be relevant to ensure the functional interface for end users resembles the current application and that APIs to other applications of the customer remain functional. Furthermore, the customer needs to consider which functions of its on-premises application have been used and if these are available on the target platform of the CSP. Examples are customers moving from on-premises MS Office to cloud based Microsoft 365, which is rather seamless as the functions are comparable. However, if the customer moves from on-premises MS Office to Google Workplace in the cloud, it needs to consider the functionality offered. The migration planning should therefore consider end user training, amendments of APIs and/or changes in business processes. In this scenario, data portability (in particular data syntax and semantics) is important. Tools may already be available to address this challenge. However, if there are differences in data semantics, this may represent a larger challenge.

5.2.2 Customer links in-house capabilities with cloud services (hybrid cloud, scenario 2)

The second scenario is where a customer has first added cloud services stand-alone and later on decided to link the in-house application with the cloud services. This is very relevant as customers increasingly consider how to leverage their existing in-house IT investments alongside their newly adopted cloud services or are still in the middle of the deprecation cycle of the old on-premises investment. One of the most important use cases is where the enterprise customer keeps their Identity and Access Management on-premises, giving them the freedom to make use of multiple cloud services while maintaining centralised control of access and credentials.

The approach differs depending on the cloud service model:

- When linking on-premises applications and IaaS cloud services, the customer is responsible for addressing functional integration as it controls all the interfaces used by its applications. For IaaS, the control logic of the application is in the on-premises part of the solution but using Virtual Machines (VMs) is more cost effective in the cloud. Thus, the control logic of the CSP is an important component for the customer to consider before migrating part of its workload to this new environment. In this case, there is no need to change the application code, but the system operation scripts need to be modified to instantiate the required VMs in the cloud.

- Linking on-premises applications to PaaS cloud services, requires identification of the functions and data of the on-premises application, which are needed by the cloud service. Then for each of these, an API needs to be defined, which can involve considerable effort.[76] For PaaS cloud services, the customer should address most of the functional integration requirements as the application code running in the (PaaS) cloud is controlled by the customer. However, a CSP might provide assistance with tools. In addition, these APIs and/or data access imply security risks and the customer must consider how these can be addressed (Access control, firewall configuration, encryption techniques etc.). Platform providers typically provide reference material to support this step.[77]

- For linking on-premises applications to SaaS cloud services, the CSP is mainly responsible for addressing functional integration via APIs. However, it should be borne in mind that the customer's decisions regarding its current IT system, security and applications, taken over many years, result in a unique combination. The migration of certain tasks or operations to the cloud is only possible when these fit the standardised cloud applications.[78]

- As regards data portability between the on-premises application and the cloud solution, the customer maintains control for IaaS and PaaS. For SaaS, the CSP arranges the seamless integration. Examples are linking MS365 to existing on-premises MS Office applications or linking database related applications, where the customer is already using a certain database like SQL server or Oracle server.

5.2.3 Customer uses cloud services from multiple CSPs (multi-cloud, scenario 3)

In this scenario, a customer decides to use one or more cloud services from CSP A and one or more from CSP B. The services used from the different CSPs may have very different functionality (customer choosing the best cloud service for a specific area) or might be equivalent (e.g. in order to secure resilience, due to acquisition of another company, or issues regarding availability or compliance with legal requirements in different jurisdictions).

- As a baseline, it may be relevant to have interoperability for Identity and Access management. Furthermore, common admin and security interfaces may be needed to enable centralised control of the cloud services to avoid duplication of efforts and to synchronise security.

---

76 Depending or not whether the on-premises and cloud service are using Service Oriented Architecture (SOA), which is a software development model focused on integration, whereby services are allowed to communicate across different platforms. See https://www.techtarget.com/searchapparchitecture/definition/service-oriented-architecture-SOA

77 Examples are Azure Architecture Center, see https://docs.microsoft.com/en-us/azure/architecture/ and AWS Well Architected Framework, see https://innovations-on.com/blog/1x1-cloud-journey/

78 Only by standardising the application functions, cloud applications can be offered to the broadest set of customers, leading to the most economic scaling of the application.

- Interoperability at first glance seems mostly relevant for services with comparable functionality and/or business area as the likelihood of interactions would be greater. However, different applications might also require some form of interoperability (irrespective of whether or not provided in the cloud). For example a database and a financial package are very different applications, but interoperability (i.e. the "ability to communicate”) between them might still be important.
- An example of this scenario for IaaS could be the potential to access overflow/back-up capacity from a different CSP. When using different IaaS cloud services: interoperability would require a common understanding between the two infrastructure cloud services in respect to the communication infrastructure used and the structure of exchanged information. Furthermore, at semantic level, the two cloud services should have a common understanding of the data models such as virtual machines and containers, which are used to separately run the customer’s applications.[79] Data portability is usually not an issue for IaaS as the customer controls the data syntax and semantics of the application/workload
- An example of this scenario for PaaS could be the use of different CSPs for database hosting as back-up. When using different PaaS providers for back-up purposes, the customer would likely choose similar databases to avoid application portability issues and differences in data format and structure. As an example of the impact of using different databases; If the customer chooses to exploit very detailed functions of a certain database such as MySQL, then the porting of the customer-built application on MySQL to another database such as IBM DB/2 or Oracle DB is much more complex, or even impossible. Thus, if the customer values interoperability and data portability, it is best if they rely on common database functionalities to avoid portability issues. Application portability is important; not only because the same application is deployed to both (PaaS) cloud services (with different databases), but also since developers want to use the same knowledge and tools (e.g. by using a standard VM image format) in both cloud environments.
- When using multiple SaaS providers, it may be that some data from application A is required for application B. In this case it would be ideal that data has the same structure and semantics. When not, data transformation may be required to be used in both cloud environments.

79 A virtual machine and a container have the same purpose: to run an application in isolation while sharing processing and storage capacities. VMs have separate applications, bins and libraries and guest operating systems, where multiple containers share the operating system level architecture, which makes them more lightweight. See https://www.freecodecamp.org/news/a-beginner-friendly-introduction-to-containers-vms-and-docker-79a9e3e119b/

Available solutions for multi-cloud:

- Large, standardised Enterprise Resource Planning (ERP) applications like SAP are available in multiple cloud environments. The same applies for Operational Support Systems (OSS), which support the standardised business processes of customers. However, more generally the standards setting process to reach interoperability at application level requires strong engagement from amongst a variety of developers and end-users and is not fully under the control of CSPs.

Limitations on the use of multi-cloud

- Multi-cloud use can bring benefits such as resilience and the ability to leverage the best aspects of different cloud platforms for specific services. However, there are also limitations: Due to latency issues, customers could be inclined to procure infrastructure cloud services, used to support a specific application, from one CSP. This may in particular be the case when they need higher performance requirements such as for AI or where a large dataset needs to be accessed by an application. Multi-cloud solutions can also increase security risks as security solutions would need to reflect the "lowest common denominator" amongst the services provided.

5.2.4 Customer links one cloud application to another cloud service (e.g. vertical interoperability, scenario 4)

In this scenario the customer uses two cloud services, whereby one service provides input for the other as each provide specific capabilities. Almost all cloud native applications are built on software architectures and standards like REST[80], XML and Json[81] to facilitate exactly this use case. Examples are that Google maps is included in websites, using the routing algorithm to optimize fleet management or the usage of other third-party components like payment functions.

Another example is a SaaS application supporting the customer's business processes, whereby the output is then used for a custom data analytics tool on a PaaS cloud service. In this example, following aspects should be considered:

---

80 Representational State Transfer (REST) is a software architecture The advantage of REST is that the WWW already has a large part of the infrastructure required for REST (e.g. web and application servers, HTTP-capable clients, HTML and XML parsers, security mechanisms) and many web services are REST-compliant per se. Source. Wikipedia, https://de.wikipedia.org/wiki/Representational_State_Transfer

81 JavaScript Object Notation (JSON) is an open standard file format and data interchange format that uses human-readable text to store and transmit data objects consisting of attribute–value pairs and arrays (or other serializable values). It is a common data format with diverse uses in electronic data interchange, including that of web applications with servers. Source: Wikipedia, https://en.wikipedia.org/wiki/JSON

- The cloud service receiving data input should have a well-defined API that the first cloud service can use. Furthermore, network constraints linking the two cloud services should also be considered.
- If the involved cloud services are IaaS cloud services, the applications can either belong to the customer or to a third party developer. In the first instance, the customer can enable the use of the API between them. In the second instance, it depends on the third party, which might involve license conditions and support contracts.
- If a PaaS service is used, the customer uses prefabricated components (from the CSP) to write its application. This significantly simplifies application development compared to a situation where the customer writes everything themselves. This is one of the key reasons why start-up companies have been faster to adopt PaaS cloud services compared with companies which have developed their applications in programming languages themselves over a longer timeframe. Arranging interoperability and data portability for traditional ‘code based’ applications is more cumbersome than for modern PaaS based applications.
- If one of the cloud services is however a SaaS service, the application code belongs to the CSP and the APIs required for the downstream application may need to be standardised.

This scenario is also relevant in cases where an application provider seeks to build an add-on to an existing cloud service and make it available to end-users. In this case, continued functioning of the specific add-on ideally requires coordination between CSP and application provider and standardised APIs. This requires willingness from both sides to guarantee ongoing interoperability and could be categorised as vertical IOP.

5.2.5 Customer switches between CSPs (scenario 5)

This is the scenario where a customer uses a CSP for a certain cloud service and wants to switch to another CSP which provides an equivalent cloud service, which is either better suited to the customer and/or better priced. The switching scenario could be seen as migration (see scenario 1) followed by contract termination. The cost to the customer of switching can be viewed as ‘exit’ or ‘migration’ costs and, added to the procurement costs and the ongoing costs, contributes to the total cost of ownership of using a cloud service.

The admin and security interfaces of the current and new cloud service should ideally be compatible in order to continue the monitoring of applications and same security level. However, in practice, this is not always the case. Thus, the customer needs to balance (temporarily) their security versus interoperability/ data portability requirements.

The ease of migration (and time taken) depends on the layer of services at the outset and target system (with IaaS to IaaS the most straightforward), and degree to which any adjustments are needed to take into account differences between the systems and services (see scenario 1)

- For IaaS, data portability is generally not an issue as the customer controls data syntax and semantics, but for PaaS the situation is more complex as different CSP might have a different database, so the customer needs to investigate this beforehand. In practice, the larger the CSP, the higher the probability that the CSP has the customers' existing database available, which simplifies matters.
- For SaaS cloud services, the application either belongs to the CSP or a third party, but in any case, is built using the standardised building blocks of the PaaS platform of the CSP. Hence, switching implies moving from one application to another as the building blocks of CSP might differ. Furthermore, attention is also needed in relation to the interfaces and APIs to other applications of the customer. If APIs change, the customer may need to change its other applications to fit the new SaaS cloud service. This also requires that the new and old SaaS applications have identical functionality. If not, bi-directional data exchange without any data loss cannot be guaranteed. Data portability i.e. one way data transfer, is typically more straightforward especially when the data in the source and target system have the same data syntax and semantics.
- For PaaS cloud services, use of portable cloud-native technologies to develop and deploy workloads can reduce the cost of switching. New cloud-native technologies such as containers and orchestration engines allow customers to run and manage their workloads independent of choice of programming language or the run-time environment used to develop and run the application, hence providing ease of portability when the code moves to the destination PaaS provider.

The cloud industry has taken action in 2020 to establish self-regulation in respect to cloud IOP and DP via Codes of Conduct. In 2020 the IaaS Sector Group of SWIPO[82] introduced the IaaS code of conduct, with the aim to "increase CSC's confidence regarding porting and switching between IaaS cloud services or between on-premises facilities and IaaS cloud services.[83]

82 A multi-stakeholder group; SWIPO stands for Switching Cloud Providers and Porting Data. This was done in the context of the EU Free Flow of Non-Personal Data Regulation, which provides in Article 6 for self-regulation in the form of codes of conduct for all types of cloud services. This with the aim of considering best practices on switching providers and data porting. Transparency on switching processes, timeframes and charges are essential here as well as tools for professional (cloud) users to compare the services in this respect. The EC encouraged CSPs to effectively implement these codes by 29 May 2020.

83 Code of Conduct for Data portability and Cloud Service Switching for Infrastructure as a Service (IaaS) Cloud services, version: 2020-V3.0, 27 May 2020. See https://swipo.eu/wp-content/uploads/2020/10/SWIPO-IaaS-Code-of-Conduct-version-2020-27-May-2020-v3.0.pdf

The IaaS Code of Conduct acknowledges that it is difficult to estimate switching costs, but the CSP is required to provide clear information on the costing parameters for porting and switching from/to their own services. Furthermore, this Code is not a ‘one-size-fits-all solution for data portability as the approaches might vary between different cloud services.

As the Code is a voluntary instrument, CSPs have to evaluate and declare their services themselves or via third party certification. Once a service is declared compliant, the CSP must fully comply. Google for example declared on 23 June 2022 that 19 of its cloud infrastructure offerings are compliant with the SWIPO Codes of conduct.[84]

The IaaS Code of Conduct contains specific requirements for:

- Switching and porting procedures (PR01 to PR07) of which the CSP shall inform its customers
- Data porting technical measures for infrastructure Artefacts (DP01 to DP09)
- Scope of responsibilities in a transparency statement and the contract with the customer (SCR01 and 02)
- Planning requirements for performance, testing and pricing mechanism required to meet portability (PLR01 to PLR05
- Transparency requirements shall be described to potential customers (TR01 to TR06)

However, the Code excludes any compliant CSP from acting as "data controller" (only allows acting as a "data processor"), and this places most of the GDPR obligations on the enterprise customer. Also, despite the specific requirements in this code to arrange for IOP and data portability between infrastructure CSPs and/or customer’s on-premises infrastructure, it still acknowledges that the variety of technologies, protocols and methods of implementation used, as well as the customer’s on-premises facilities, may present data portability incompatibilities. Additionally, it needs to be noted that the constant innovation of cloud services, with very high numbers of functional and security updates, makes integration a ‘moving target’.

Other factors which need to be considered by the customer regarding the switching process include the following:

- Cloud agreements are often long term contracts (2-5 years) due to the need for stability and planning on both customer and CSP side. This means that the amount of data which needs to be ported, can amount to petabytes[85]. Migrating such a large amount of data requires preparation on the side of the new CSP in terms of storage but also network connection between the current

84 See https://swipo.eu/blog/press-release-google-complies-with-the-swipo-codes-of-conduct/
85 1 Petabyte equals 1 million gigabyte.

CSP and the new CSP. In practice such a migration can take between 6-12 months depending on customer requirements such as any need for continuous availability and limited downtime.

- There may be limitations on the data which can be migrated from the CSP. Data related to the customer's operational processes and/or transactions (comparable with call detail records in telecommunication) are owned by the customer and thus can be ported. However, CSPs also derive additional data as consequence of the customer consuming the cloud services. This can be observed data or inferred data based on AI and other tools, which are used to improve the CSP's services to its customers and to monitor the customer's data for which they are responsible. This observed and inferred data is typically considered by CSPs as a business secret and thus something that they consider should not be ported. Furthermore, inferred data can relate to multiple customers and therefore the movement of personal identifiable Information (PII) to another CSP could require consent from the data subjects. In addition, CSPs hold specific server and configuration data, which also belongs to the CSP.

5.2.6 Scenarios for residential consumers (scenario 6 and 7)

Although they may not view it as such, residential consumers make extensive use of cloud services including the rental of content e.g. through iTunes or storage and development of documents in the cloud e.g. Office 365 or Google Docs. These could all be described as examples of SaaS.

In this context, moving data from one cloud provider to another (in the context of switching or while maintaining both services) may be relevant.

- To achieve data portability consumers need as a minimum to be able to download and upload data. Use of standardised formats (e.g. for video encoding) and/or conversion tools can also be important to ensure that the data can be interpreted by another application. However, in some cases the formats are so different that portability into a similar format is not possible. For example, it is not possible to directly port a presentation from OpenOffice to Prezi.com, because the data structure is different (OpenOffice presentation has slides, while Prezi presentation does not).
- The ability for applications to be interoperable might become relevant in cases where consumers want to share their dataset between different cloud applications. It is unclear however to what extent there is demand for this solution and if so, in which context.

5.3 Conclusions

A review of different scenarios reflecting the typical enterprise customer journey from solely on-premise IT to the use of cloud computing solutions (including cloud-native applications) in different permutations shows that there are a number of circumstances where portability (between on-prem and cloud or between clouds) is likely to be relevant. However, it also reveals that the process can be complex. The degree of complexity depends on customers' choices about the services and degree to which they plan to outsource their management to a CSP (noting that IaaS provides the greatest degree of flexibility, but also leaves responsibility for the platform and service layer and any associated portability and/or interoperability in the hands of the customer).

For a medium to large enterprise, the process of moving to the cloud, switching to a different provider or making use of multi-cloud solutions is likely to be project-based and requires bespoke adaptation of some applications and transformation of data when migrating to alternative applications.

It should also be noted that portability in a manner which preserves all features (equivalence) is not possible while maintaining the potential for service providers to differentiate and innovate in the features provided. Interoperability, which implies the potential for continuous exchange of data, can be important e.g. between on-premise and cloud solutions and in the context of multi-cloud, but has the same limitations as portability, and thus enterprise customers which value interoperability typically build their own applications (on IaaS or PaaS) or procure from different CSPs applications with the same functionality e.g. in relation to a database or interpretation of formats. The development of global standards in relation to certain concepts (e.g. data models such as virtual machines and containers) languages and formats (e.g. JSON, XML) is important in enabling portability and interoperability, and standards such as these continue to evolve to meet market needs.

In contrast to larger enterprises, consumers and micro-enterprises generally do not engage in developing bespoke cloud services and instead purchase SaaS services directly. For these customers, portability (primarily in the form of data migration) can be important in enabling them to switch to a different provider, in particular where they have created or uploaded their own data to the cloud. This is supported by legal obligations, which require CSPs (and others) to make available consumers' data in a machine-readable format. It is also important that the conditions for contract termination should be reasonable to avoid lock-in. Commonly used standards and conversion tools can help to allow consumers to open files and documents from different SaaS providers. However, there are limitations on the degree to which consumers can maintain equivalent functionality when porting data or "switching" to a new provider, because services are unlikely to be fully equivalent and even where they are comparable, scope is needed for innovation in service functionality.

6 The impact of proposed legislation and alternative approaches

In this chapter, we summarise forthcoming and proposed EU legal provisions which could apply to cloud computing and consider the implications of these measures for innovation, competition and consumer welfare. We propose potential alternative formulations which could better target regulatory measures and avoid unintended costs. A summary of findings is provided below.

- The draft Data Act proposes a raft of obligations on cloud service providers including an obligation for the donor CSP to allow contract termination within 30 days without cost and without any minimum contract duration, and mandates CSPs to facilitate full continuity in the provision of functions and services. The Data Act also includes far-reaching obligations for interoperability and portability including a goal or requirement for functional equivalence in services.

- These proposed obligations are likely to be challenging to interpret, implement and enforce.

- Cloud computing includes a vast range of different kinds of services. Interoperability and portability is not meaningful in a generic sense, but only in relation to specific cloud services or data. Moreover, the requirement to achieve ”full equivalence“ in interoperability and ”service continuity” in switching leave little room for differentiation and innovation.

- The proposal that cloud service providers should provide 30 day contract termination and support switching free of charge is unsuited to enterprise contracts and is unrealistic, in particular for bespoke services which involve upfront investment by the enterprise or cloud service provider. Moreover, the onus on the donor to support switching misses the important role that must be played by the recipient provider, as well as the customer in what is typically (in the case of enterprise migration) a project-based exercise which does not involve swapping one service for an identical alternative. An option for 30 day contract termination may be more realistic for standardised SaaS solutions provided to consumers and small businesses, but requiring this as the only option, could limit the potential for customers to benefit from discounts for engaging in longer contract periods (e.g. of a year), and service continuity may still not be feasible when “switching” due to differences in service characteristics.

- to the draft Data Act seems to presume that regulatory intervention is generally necessary but demands for specific aspects of interoperability or portability are often addressed by the market through voluntarily adopted standardised formats and languages, conversion or migration tools.

- **Recommendation 1:** Replace blanket obligations for cloud interoperability and portability and undefined standards goals with clarification that the Commission can intervene to request standards development and/or mandate given standards for specific applications / cases where (i) intervention is necessary to meet user needs for interoperable services and/or portability; (ii) there is evidence of demand for a specific form of interoperability and/or portability that is not being met by the market; and (iii) the conditions described in Recommendation 2 are fulfilled.

- **Recommendation 2:** when considering the development and potential mandating of standards, ensure that the relevant use cases are clearly identified, intervention is relevant to the problem identified, and that the measures are proportionate and take into account the implications on innovation and the potential to differentiate. Furthermore, the objective that interoperability should achieve "functional equivalence" should be limited to *basic* functions (i.e. mature and established functions[86] which have been identified as essential) and further clarify this concept.

- **Recommendation 3**: As regards switching: in place of the unrealistic and indiscriminate requirement to offer contract termination within 30 days at no cost, and with assurance of service continuity, require cloud service providers to collaborate in good faith to facilitate porting of customer data and applications in the context of service migration. An *option* for 30 day contract termination could also be provided specifically for standardised SaaS solutions provided to consumers and small businesses, but should not be mandatory (as customers may prefer other options). Support for migration could also be offered to CSPs and their customers (in particular SMEs) by developing model contract provisions addressing certain common issues.

- **Recommendation 4:** The Data Act should avoid overlapping or adding to other legislative measures. It should focus on procedures to implement symmetric measures which are not already addressed through other symmetric instruments, or through asymmetric obligations applied under the DMA. Standardisation should involve participation and commitment from relevant sectors as a whole

86 These could be a subset of the functions available in more complex services or common functions involved in relatively standardised services provided to consumers and SMEs.

6.1 Forthcoming and proposed obligations regarding cloud interoperability, portability and switchability in EU legislation

EU legislators have proposed increasingly wide-ranging requirements on interoperability and portability in the cloud environment, reflecting Member States' preference for "completely interoperable, open, multi-vendor cloud platforms and services, based on European, international or open source standards".[87]

The GDPR,[88] adopted in 2016, established (Art 20) a "**Right to data portability**", whereby a data subject has a right to have their **personal data transmitted directly from one controller to another**, where technically feasible. The GDPR also notes (recital 68) that "***Data controllers should be encouraged to develop interoperable formats that enable data portability***."

The DMA, approved on 12th October 2022, places specific further obligations on operators which are deemed to be "gatekeepers" in relation to "cloud computing services",[89] which is defined as "digital service that enables access to a scalable and elastic pool of shareable computing resources."[90]

The DMA provides that gatekeeps should "provide end users and third parties authorised by an end user, at their request and free of charge, with effective **portability of data** provided by the end user or generated through the activity of the end user in the context of the use of the relevant core platform service, **including by providing, free of charge, tools to facilitate the effective exercise of such data portability, and including by the provision of continuous and real-time access to such data."**[91] Regarding switching, the DMA provides in Article 6(13) that "T**he gatekeeper shall not have general conditions for terminating the provision of a core platform service that are disproportionate**. The gatekeeper shall ensure that the conditions of termination can be exercised without undue difficulty."

Another requirement agreed by the EU's co-legislators in the context of the DMA concerns asymmetric interoperability for messaging platforms, which may mean that smaller platforms can request that designated core platform services enable their users to be able to exchange messages, send files or make video calls across messaging apps.[92]

---

87 https://digital-strategy.ec.europa.eu/en/news/towards-next-generation-cloud-europe
88 https://eur-lex.europa.eu/eli/reg/2016/679/oj
89 Cloud computing is listed under Article 2(2) as a "core platform service"
90 Article 4(19) Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.
91 Article 6(9) DMA
92 Europe says yes to messaging interoperability as it agrees on major new regime for Big Tech | TechCrunch

The provisions in Article 6 and 7 of the DMA can be further specified through the adoption of an Implementing Act by the Commission,[93] a provision which may be an acknowledgement the real challenges that may arise in interpreting the provisions in the very differing range of scenarios and services for which they could in theory be applied.

More specific provisions regarding interoperability and data portability for cloud services have been put forward in the context of the proposed Data Act, released in 2022, in particular in Chapter VI, which concerns switching between data processing services. Providers of data processing services are required inter alia, to provide for **contract termination within 30 calendar days**, and enable porting of data applications and other digital assets to another provider of data processing services (or to post to an on-premises system) also within 30 days. The data processing service provider should assist in the switching process and ensure **full continuity in the provision of functions and services**. The data to be ported should include **data and metadata created by the customer and by the use of the service including configuration parameters, security settings, access rights and access logs to the service**. An exemption from the 30-day technical transition process is possible if this transition is not technically feasible, but in this case the reason must be duly motivated and an alternative transition period of a maximum of 6 months must be offered. **Switching charges must be reduced initially to cost-based levels before eventually being eliminated**. In certain provisions (article 26), a distinction is made between switchability for IaaS, which should allow "functional equivalence" in the use of the new service and for downstream portability, and for PaaS/SaaS for which there is a **requirement to make available open interfaces publicly available and free of charge and to comply with standards and specifications on interoperability**. These open interfaces should be compatible with European standards or (where standards are not available) data (including formats and structures) should be made available in a commonly used and machine-readable format.

According to Article 29 of the draft Data Act, the standards and specifications on interoperability should (article 29 (1) c), guarantee, where technically feasible, functional equivalence between different data processing services that cover the same service type. Open interoperability specifications and European standards for the interoperability of data processing services should address:

> (a) **the cloud interoperability aspects of transport interoperability, syntactic interoperability, semantic data interoperability, behavioural interoperability and policy interoperability**;
>
> (b) **the cloud data portability aspects of data syntactic portability, data semantic portability and data policy portability**;

---

93 Article 8(2) DMA

(c) **the cloud application aspects of application syntactic portability, application instruction portability, application metadata portability, application behaviour portability and application policy portability**.

Further definitions are applied for "application portability" which refers to the ability to migrate an application from a source system to a target system. This includes metadata portability and instruction portability whereby the application's instruction set executes on the target.

As justification for the Commission's involvement in this space, the proposed Data Act notes (recital 76) that "*As **market-driven processes have not demonstrated the capacity to establish technical specifications or standards that facilitate effective cloud interoperability at the PaaS (platform-as-a-service) and SaaS (software-as-a-service) levels,*** *the Commission should be able, on the basis of this Regulation and in accordance with Regulation (EU) No 1025/2012 (concerning Standardisation), to request European standardisation bodies to develop such standards, particularly for service types where such standards do not yet exist*."

6.2 Observations on proposals for interoperability and portability

A first and overarching point is that, as described in previous section, the scope of proposed (assumed horizontal) interoperability and portability obligations has expanded over time and is particularly wide-ranging in the draft Data Act. **The proposal seems to seek to impose horizontal interoperability and switching obligations (including mandatory timeframes) for all use cases of data processing services without assessing the practicality of these measures or identifying the specific problems that they are designed to address**. It is surprising in this context that the provisions of the Data Act, which are intended to apply to all CSPs go much further than those applied to "Gatekeeper" CSPs, which are required under the DMA to provide tools to facilitate data portability and to ensure that the conditions of termination can be exercised without undue difficulty. Meanwhile interoperability obligations under the DMA apply only to relevant Core Platform Services in which "gatekeeper" status has been found and is described as a condition that is "susceptible to further elaboration".

A more detailed examination of horizontal interoperability in particular, as well as switching processes in relation to cloud shows why it is not realistic to impose blanket obligations as envisaged in the Data Act.

A first concern is that the Data Act fails to consider in which circumstances horizontal interoperability or portability may be relevant. A key point is that **horizontal interoperability and switching is not meaningful in a generic sense, but only in relation to specific cloud services or data**.

Customers may value the ability of one service to be able to open and process content produced in another similar service. However, **it may not always be necessary to intervene.** Demands of this kind are often addressed through voluntary measures to standardise certain file formats, use common languages or provide tools which aid conversion. *Mandating* standards could also have a perverse effect as larger players may be better equipped and resourced to engage in the standardisation process, and smaller players may face disproportionately higher costs in participating and adapting their products and processes to meet the standards. Moreover, in some cases, customers may not expect or require the ability to switch seamlessly between services.

The Data Act proposes that standards and specifications on interoperability should seek to achieve "**functional equivalence**" and that the donor CSP should facilitate "**full continuity**" in the provision of functions and services following a decision by the customer to switch to another provider. However, these far-reaching requirements **would limit the potential for service differentiation and innovation,**[94] thereby limiting choice for end-users. The implications for innovation can be seen from the case studies in section 4.3, which show that horizontal interoperability helped to cement the role of telephone calls, basic banking services, SMS and email as basic and essential services. However, innovation in these services was essentially frozen and instead evolved in the space that was left unregulated e.g. through online messaging, social media and video calls. This effect was foreseeable in view of the fact that the lengthy process to develop standards itself tends to deter innovation, while investment in developing innovative new services is deterred if this innovation would immediately be subject to standardisation (effectively removing the first mover advantage that would normally be enjoyed by the innovator).

More generally, in seeking inspiration for horizontal interoperability and portability/switching from sectors such as telecoms and banking, the **Data Act fails to reflect the significant differences between telecoms and banking and cloud computing**. Establishing conditions (including deadlines) for switching (including number portability) makes sense in the context of telecoms and banking because the services themselves are uniform, they are considered essential (and used by the vast majority of consumers), and most customers "single home" i.e. they use one provider as their main or only provider. However, cloud computing involves a much more diverse set of applications and data than that relating to phone calls and numbers or banking identifiers and key transactional instructions. Moreover, the nature of the services and the way they are used differs. Cloud computing is not "universal" in the same sense as banking or telephony, and customers frequently multi-home.

---

94 Different considerations apply with respect to vertical interoperability, as this can foster innovation by enabling customers and other application providers to innovate on top of a platform or service. The implementation of vertical interoperability has led to innovation in the banking sector as well as in software, and promises to achieve positive results in relation to healthcare, through the European Health Data Space initiative. However, it is also **unlikely that a blanket obligation regarding "vertical interoperability" for cloud services will be effective** because opportunities for "over-the-top" service development are case specific, and are likely to require specific inputs, as can be seen in the banking example. Moreover, there is **no need to pursue regulatory solutions, unless there is a market failure which serves to stifle innovation.**

Porting of cloud-based applications and data, sometimes accompanied by switching remains relevant. However, the examples in section 5.2 illustrate that the processes for achieving this – in particular for enterprises – are not straightforward, and depend on the choices of the enterprise concerned, the nature of the applications and the volume of data, which can be significant. Except for very simple transfers e.g. between identical platforms and/or software provided by different cloud providers, it is inevitably a **project-based process, which is very likely to take more than the 30 days** which is proposed to be required in the draft Data Act. Moreover, migration of applications and data is likely to incur cost for both parties and in situations where significant investments have been made by the CSP to provide bespoke solutions for (and sometimes in conjunction with) enterprises, it may not be reasonable to expect that migration should be offered without cost or that it is realistic to terminate a contract within 6 months, noting the sunk costs incurred. Rather, the **notice period and costs and conditions associated with the provision as well as the termination of the service, and support for migration would normally be included within the bespoke contract** signed between a CSP and the enterprise customer, which should take these factors into account when comparing different offers and in deciding to what extent they wish to tailor the service to their specific needs.

For individual consumers and micro-enterprises making use of standard SaaS applications, porting data may be more straightforward and access to data should be provided in a relatively short timeframe. This facility is already available from most major cloud providers, and standards could be further developed for essential and common functions or data required for porting. An option could also be provided for contract termination within 30 days for standard SaaS services provided to consumers and small businesses to limit the risk or perception of lock-in. However, it should be noted that **porting and the concept of "switching" is only relevant between similar types of services and the degree to which the consumer can expect to be able to receive an equivalent service after switching, depends on the degree to which the old and new provider offer the same functionality, and thus cannot be guaranteed**.

While well targeted and well thought-out standards such as Bluetooth and IoT (Matter),[95] can contribute to innovation and create a wider market for innovation by participating companies, requiring all cloud services to be **so standardised that it is possible to port all applications and data within 30 days allowing equivalent functionality would limit innovation**, because all applications would need to be understood and interpreted and run by all platforms, and all data would need to be understood and interpreted by all applications. In addition, requiring the new service to deliver not only the same output but also the same performance and the same level of security, operational resilience and quality of service could limit the scope for the customer to choose alternative (including reduced) functionality e.g. if such functionality is not needed or is considered too costly.

95 https://csa-iot.org/all-solutions/matter/

Limiting the potential for differentiation and the scope of the customer to choose cannot have been the intention of the legislators.

There are also questions around who should take responsibility for the switching process. The draft Data Act proposes an obligation on the donor provider to ensure "full continuity" in the provision of functions and services during the switching process. However, **effective migration can only be achieved through co-operation between the donor and recipient provider with the approval of (and in the case of enterprise services sometimes extensive involvement of) the customer**. The need for joint responsibility between the donor and recipient is recognised in the procedures commonly put in place to support number portability in the telecom sector, which provides an example of a relatively straightforward form of portability.

The obligation to remove all commercial, technical, contractual and organisational obstacles to switching is very broad and could have a variety of interpretations (and implications for cost and timing), noting the breadth of the services that could be potentially covered by this provision.

In this context, it should be noted that switching between a source and a destination service will always involve some cost and effort. When the two services are very similar, and data can be easily extracted from the source provider and be transferred to the destination, the cost and effort could be small. But in many real-world scenarios, especially when the service involves porting application code, or when the data may need to be modified to be usable by the destination service, the cost and effort required may not be negligible. The stakeholders should all work together to put best practices in place in order to reduce the cost and effort involved. Use of industry-wide standards or well documented data formats, when possible, is one such measure to manage the cost.

6.3 Recommendations for policy makers

Drawing on our analysis of the nature and demand for interoperability and portability in cloud computing and the implications of the proposed legislative measures, we derive the following recommendations for policy makers with respect to the Data Act.

Recommendation 1: instead of including blanket obligations / goals for interoperability and portability, clarify that the Commission should have the power to intervene in specific situations/use cases where certain conditions are met.

Interoperability and portability obligations or goals to set interoperability standards in relation to the "cloud" make sense only in the context of specific use cases. Instead of overarching requirements for CSPs to achieve interoperability and portability across all dimensions and levels of the value chain (which is likely to be challenging to interpret, implement and enforce), the text should be amended to clarify that the European Commission is empowered to require relevant industry bodies to develop standards and/or to make existing or new cloud computing standards mandatory, in relation to specific cases where this would be necessary to meet end-user needs for interoperability and/or portability, and there is demand for specific types of interoperability and/or portability that is not being met by the market (i.e. where there is a market failure). In this context, regulators should assess the degree to which customers can already multi-home at low cost, and whether commercial solutions exist or are being developed to address the perceived problem. Regulators should also be required to ensure that any obligations are relevant to the problem identified and proportionate, and that the conditions set out in Recommendation 2 are met.

Recommendation 2: take into account the implications of interoperability and portability on innovation and the potential to differentiate.

It should be clarified that any standards mandated in this field should take into account the need to preserve incentives for innovation and the potential for service providers to differentiate their services and for CSPs and end-users to benefit from such differentiation. The objective that interoperability should achieve "functional equivalence" should be dropped or limited to basic functions or data points (i.e. a subset of mature and established functions or data points which have been identified as essential), and it should be acknowledged that delivering the same performance, security levels, operational resilience and quality of service may not be technically possible and even where technically feasible, could undermine the principle of competition in service provision, limiting customers' ability to choose freely from different options (including lower cost and potentially less performant solutions for less business critical applications).

Recommendation 3: as regards switching, distinguish conditions for enterprise services from standard services, facilitate switching through an obligation on cloud service providers to collaborate in good faith to facilitate porting of customer data and applications in the context of service migration, limit the option for 30 day contract termination to standard SaaS services provided to consumers and small businesses and consider developing model contract provisions to aid CSPs and SME with common issues that relate to migration.

The provisions of the Directive on switching should be amended to reflect the fact that migration within 30 days free of charge is not realistic in particular for enterprise customers and does not reflect the complexities and cost that may be involved in these migration processes. Moreover, it should be recognised that even for more basic services offered to consumers and SMEs, requiring 30 day termination may limit the potential for discounts (e.g. if a customer subscribes for 1 year). Moreover, a general obligation to maintain continuity of service during migration cannot be achieved unless services are fully equivalent.

The current unrealistic proposed obligations regarding switching timeframes and cost could be replaced by a general requirement that donor and recipient service providers should collaborate together with customers to facilitate data porting and migration, to the extent technically and economically feasible. In parallel, the Commission and relevant industry bodies could usefully develop model contracts which provide guidance in particular for smaller companies on provisions regarding contract termination and processes for migration. Unlike telecoms and banking, where the use case is clearly defined and underlying processes are understood, we do not recommend the inclusion of generic deadlines in the legislation for porting or switching in the context of cloud or general requirements that such processes must be provided free of charge. However, where objectively necessary, specific deadlines, processes and cost attribution principles could be established via implementing measures for specific (well defined consumer) baseline use cases following due process including the involvement of industry groups and/or standardisation bodies. Likewise, the categories of data that should be susceptible to porting cannot readily be defined for cloud computing generally through legislation. It may be more realistic and appropriate to require in general terms that data should be provided to the extent that it is necessary to make use of the service of the recipient CSP, and leave the types of data to be provided (and if needed specific data points) to be specified on a case specific basis (through implementing measures), where needed.[96]

Recommendation 4: The Data Act should avoid overlapping or adding to other legislative measures. It should focus on procedures to implement symmetric measures which are not already addressed through other symmetric instruments, or through asymmetric obligations applied under the DMA. Standardisation should involve participation and commitment from relevant sectors as a whole.

The DMA includes procedures to designate cloud providers as gatekeepers and specify “asymmetric” obligations to address problems linked to this gatekeeper status. Horizontal measures are already being taken through other legislation to address interoperability needs for certain basic data in essential industries such as banking and health, and the DMA includes requirements relating to portability/switching on CSPs found to be gatekeepers. Bearing this in mind, the Data Act should avoid overlapping or additional regulation and rather provide procedures to address on a “symmetric” basis (i.e. on all service providers) issues that are not covered elsewhere (including through the DMA). In turn, if the Data Act is used to provide the means to mandate standards applicable to all cloud providers, care is needed to properly target and specify any obligations and ensure that they are justified and proportionate (see Recommendation 1). Processes should also be discussed, and if possible, agreed by a range of participants within the sectors involved, noting that all parties need to be involved (not just the donor CSP) in any implementation of porting or interoperability for a given use case.

96 For example, metadata is a commonly used term, but its interpretation is not always clear. It could for example be CSP generated or CSC generated depending on the circumstance. Moreover, while "configuration parameters, security settings, access rights and access logs", can sometimes be relevant to customers, in some cases these data elements may be relevant only to the CSP.