Centrum für Europäische Politik
FREIBURG | BERLIN

cep**Study**

European Leadership in the Digital Economy

Seventeen Recommendations

This study by the Centre for European Policy (cep) has been commissioned by SAP. The opinions expressed in this study are those of the authors and do not necessarily represent positions of SAP.

Authors:

Dr. Bert Van Roosebeke

Dr. Martina Anzini

Philipp Eckhardt

Anne-Carine Pierrat

Freiburg, February 2020

Corresponding Author:

Dr. Bert Van Roosebeke

cep | Centre for European Policy

Head of Division

Kaiser-Joseph-Strasse 266 – D-79098 Freiburg

+49 (0) 761 – 386 93 230

vanroosebeke@cep.eu

cep | Centre for European Policy

Kaiser-Joseph-Strasse 266 | 79098 Freiburg | Germany

Phone: +49 761 38693-0 | www.cep.eu

cep is the European policy think tank of the non-profit organisation Stiftung Ordnungspolitik. It is an independent centre of excellence specialising in the examination, analysis and evaluation of EU policy. The offices of cep are located in Freiburg, Berlin and Paris.

EXECUTIVE SUMMARY

This study identifies three main priorities and seventeen detailed recommendations for a European political agenda aiming to reach European leadership in the digital economy. Setting priorities is urgently necessary. Europe is lagging behind the United States and China in artificial intelligence and cloud computing, two of the main global technical trends which will seriously affect economic growth in the years to come.

Whereas network effects and economies of scale have led to an American and Chinese dominance in B2C-markets, the EU should now take the necessary actions to avoid the same happening in B2B-markets.

Protectionism measures are not helpful in regaining European technological sovereignty. On the contrary, the three priorities all have a market-oriented approach, spurring innovation and safeguarding competition amongst suppliers in the digital economy.

As a **first priority**, the EU should actively foster a true internal market for data as the EU is not nearly using the economic potential associated with the sharing and (re-) use of the data present in its territory. Actions in this field should concern personal, public and non-personal data.

Regarding personal data, we plead for more harmonisation and the use of sandboxes and regulatory hubs to create legal certainty in applying the GDPR.

The availability of public data should be increased through standardisation of data formats, through the inclusion of data availability as a factor in public procurement and through stricter data-access rules for public data of high-value.

Reasons why businesses are hesitant in sharing and pooling non-personal data are very diverse and not all of them can be solved through policy action. The EU data space initiative can however contribute to lowering transaction costs of B2B data sharing.

National data localisation requirements concerning the storing of personal, public or non-personal data hinder the realisation of economics of scale and are generally incompatible with the very idea of an internal market for data. They should remain the exception and we call upon the Commission to consistently proceed against localisation requirements that are not justified under the GDPR and the FFD-Regulation.

As a **second priority**, the EU should ensure effective competition on digital markets in the B2B-sphere. B2B-markets are markedly different from B2C-markets and we do not see a wide-spread need for regulatory action to safeguard competition. In the field of cloud activities, vertical integration and limited access to infrastructure on the different layers of the market (IaaS, PaaS and Saas) might be able to limit competition in the future. Competition law can handle such problems and sector-specific regulation is not needed. On the same markets, limited access to essential data may also limit competition. In these cases, regulatory interventions aiming at ensuring data portability on cloud markets may be necessary. In any case, such intervention should be targeted to operators with a market dominant position only.

The **third priority** concerns a European digital industrial policy and focusses on the general competitiveness of the European digital economy as a precondition for digital sovereignty. The digital industrial policy should protect the openness of the economy, allow for economies of scale, entail investment friendly infrastructure regulation and promote digital skills.

We propose a EU Framework for secure and trusted cloud computing as a main element of such a digital industrial policy. The framework addresses concerns related to data security, data governance and service availability in the cloud. Those concerns go back to the widespread use of non-European hyperscalers by EU companies and reflect the public good character of cloud service availability to our economies and societies.

The proposed framework is proportionate, efficient and non-discriminatory. It defines certification schemes for the voluntarily classification of cloud service providers on the basis of the EU Cyber Security Act. Following that, we propose a governance structure that guarantees a safe use of cloud services by a limited number of operators of essential services such as financial services, energy or transport throughout the EU. Most importantly, our proposal aims at avoiding any competitive distortions between private providers of such essential facilities.

17 Recommendations to promote European leadership in the digital Economy

NINE RECOMMENDATIONS FOR A SINGLE MARKET FOR DATA IN THE EU

- **Recommendation No. 1:** The Commission should keep on **monitoring closely** the evolution of the **market of data trusteeship** to timely detect the emergence of any future obstacle preventing the business from going cross border.

- **Recommendation No. 2:** The European Commission should use the upcoming review of the **GDPR** to ensure **legal certainty through a higher level of harmonisation**.

- **Recommendation No. 3:** Initiatives that aim at increasing **legal clarity in the GDPR** by establishing a dialogue between Data Protection Authorities (DPAs) and businesses or innovators are **to be supported**. They can help DPAs to identify new developments in technology and innovation while ensuring that people's rights to privacy and data protection are respected. At the same time, these initiatives, whether called **"sandboxes" or "regulatory hubs" must be market neutral** (i.e. available to all market participants).

- **Recommendation No. 4:** The Commission should develop, together with the relevant stakeholders, **open standards on platforms and data formats for public sector bodies** to make available their data. The standardisation should be carried out on a sectoral basis.

- **Recommendation No. 5:** The Commission should aim to **extend the scope of the PSI Directive to include private companies providing public interest services**, thus ensuring the availability of privately held data relating to the provision of the public interest service. The Commission should also encourage Member States and their public authorities to make public procurement conditional upon the availability of data generated in this context.

- **Recommendation No. 6:** The Commission should investigate whether establishing a **general obligation to grant access to public sector data and public interest data** might be necessary, first and foremost **for high-value datasets**. It should especially look into the existing data sharing practices of public and private companies in particular sectors – e.g. transport, geospatial – to evaluate if data sharing based on voluntary agreements is sufficient or if further action – be it through soft-law measures or binding EU law – is required.

- **Recommendation No. 7:** The European Commission's European **data space initiative may contribute to reducing transaction costs of B2B data** sharing in Europe. The initiative deserves to be intensified as long as it is market-neutral by design.

- **Recommendation No. 8:** A **legal ownership right to data should not be introduced**. De facto control over data through contract law and technical restrictions form a sufficient basis for data market development.

- **Recommendation No. 9:** As data localisation requirements hinder the development of a single market for data in the EU, the EU-Commission should consistently **proceed against national data localisation requirements** that are not justified under the GDPR and the FFD-Regulation. In order to enable the identification of data localisation requirements under the GDPR, the possibility of installing a register for national data localisation requirements under the GDPR should be investigated.

FIVE RECOMMENDATIONS TO MAINTAIN EFFECTIVE COMPETITION ON CLOUD AND DIGITAL MARKETS

- **Recommendation No. 10:** The market for large scale cloud services (**hyperscaler market**) is currently characterised by intense competition amongst a relatively small number of competitors facing high fixed costs. It remains to be seen whether the current level of competition will prevail also in the future. In any case, any **public intervention** – e.g. by regulating switching-costs between cloud providers, interoperability requirements or end-user-prices – which is **motivated by competition concerns should take place only given proof of a significant and non-contestable market power** (SMP) of a cloud service provider. Upon proof of such market power, competition law seems well able to offer an appropriate answer. The use of **sector-specific regulation** addressing dominant cloud service providers is **not recommended**.

- **Recommendation No. 11:** Whether or not a PaaS-provider holds significant market power has to be investigated on a case-by-case basis. In any case, **the finding of a non-contestable market dominance of a platform provider should be a pre-condition for competition-based intervention.** If proven, such dominance can be dealt with appropriately using general competition law. **A need for sector-specific regulation is not evident.**

- **Recommendation No. 12:** Tying and bundling practices by **cloud providers vertically integrating into the PaaS-market** are unproblematic, unless those providers hold a non-contestable market power on the cloud-markets. If they do, **competition law** is well fit to cope with this abuse behaviour.
  Absent tying and bundling, the **refusal** by a vertically integrated cloud provider **to grant** PaaS-competitors **access** to its cloud infrastructure **can be dealt with using** the essential facilities doctrine. This doctrine offers a convincing trade-off between protection of intellectual property rights and competition on aftermarkets. The need for intervention is limited to cases where the following criteria are fulfilled: (1) the cloud provider holds a non-contestable dominance on the cloud market, (2) the use of the cloud is imperative, (3) competing PaaS-providers offer a novelty and (4) the cloud provider cannot offer objective reasons justifying the refusal of access. Although a sector-specific access regulation regime may be able to cope with dominant, vertically integrated cloud providers on the PaaS-market, clear advantages of such regulation as compared to **general competition law** are not apparent.

- **Recommendation No. 13:** Privileged data access may hinder competition. **On the SaaS-market, the vertical integration of IaaS-providers down to the PaaS and SaaS-markets** and the associated market concentration **may** aggravate the competition problems on the SaaS-market associated with privileged data access. Also, privileged access to data may **cause competition problems** in very different downstream markets.

With the essential facilities doctrine, **competition law** offers a sound fundament to deal with competition issues in respect with vertical integration. However, in practice, if data turns out to be the essential facility, access-granting **may prove** to be very **difficult and unpractical.** In that case, alternative remedies or **regulatory interventions** that prevent data being or becoming an "essential facility" **may be necessary**. Such interventions **should aim at increasing data portability**, be it by lowering barriers to switching and preventing lock-in situations or by granting direct portability rights.

However, when doing so, **intellectual property rights** must be given due consideration. In any case, the finding of a **dominant market position** in the absence of potential competition on a well-defined upstream data market must be a **precondition for any intervention**. In cases where markets are defined very narrowly (e.g. brand-wise), the finding of market dominance may be rather straight-forward and regulation may be appropriate. In all other cases, competition law can better guarantee an appropriate market definition and analysis of market dominance.

- **Recommendation No. 14:** The most appropriate tools to **grant legal certainty** in questions of anticompetitive behaviour **concerning data pooling** are:
  - the **guidelines** of the Commission because, by identifying significant circumstances for the application of Article 101 TFEU to data pools agreements, they can be relied upon by undertakings while self-assessing their market behaviours;
  - the **guidance letters**, because the level of change brought about by Big Data in competition law analysis is so massive that genuinely novel questions are likely to arise. This would enable the related applications for guidance letters to be finally upheld by the Commission.

THREE RECOMMENDATIONS FOR A EUROPEAN DIGITAL INDUSTRIAL POLICY

- **Recommendation No. 15:** Attaining a **competitive European digital economy is a conditio sine que non for digital sovereignty.** The bulk of the work and investment to reach this aim has to be delivered by private investors and the private economy. Nevertheless, the EU, national legislators and policy makers should set the appropriate regulatory framework for this to happen. This framework should (1) safeguard the openness of the economy and (2) competition, (3) allow for economies of scale, (4) entail investment friendly infrastructure regulation and (5) promote digital skills.

- **Recommendation No. 16:** The EU, through the Commission, should negotiate an **agreement with the US** which clarifies the rules regarding cross-border access to electronic evidence in the context of criminal proceedings. Not only should this agreement protect EU citizens and companies by ensuring the necessary safeguards, but it should also aim at increasing legal certainty in data access requests by US judicial authorities to EU service providers, thus preventing conflicts of law.

- **Recommendation No. 17:** We propose an EU Framework for secure and trusted cloud computing that addresses concerns related to data security, data governance and service availability in the cloud. The growing use of cloud services brings about a lot of economic advantages, but at the

same time confronts us with political and operational risks which may endanger the continuous availability of services which are essential to our economies. The public good character of cloud service availability justifies public intervention.

We propose the creation of an EU Framework for Secure and Trusted Cloud Computing as a model of public intervention regarding the use of cloud services which is proportionate, efficient and non-discriminatory. It consists of three steps.

- **In Step 1**, the EU should define common requirements for secure and trusted cloud computing that will address user concerns related to data security, data governance and service availability. As requested by the European Commission, the ENISA should draft baseline cloud computing security certification schemes regarding general use. In addition, ENISA should draft complementary cloud computing security certification schemes for public administrations and sectors providing essential services (according to the NIS-Directive).
- In **Step 2**, the existing modalities for the issuing of certificates in the Cybersecurity Act can be applied to the certification of cloud service suppliers without any change. There is no need for making certification compulsory.
- In **Step 3**, the use of cloud services by economic actors in certain sectors can be made conditional upon the use of a cloud provider of a certain assurance level of the cloud security certification schemes. Any such regulatory requirements must be risk-based, proportionate and may not distort competition, neither between cloud service providers nor between regulated entities.
- In order to reach a uniform application of these regulatory requirements, we recommend in **Step 3a** a consistent identification of essential service operators to whom regulatory requirements will apply. For this reason, we propose a more formal role for the NIS-Directive's "cooperation group" to identify operators from the energy, transport and financial market sector (but not for banks).
- After confirming in **Step 3b** that cloud security requirements for essential service operators will follow the EU cloud security certification scheme, it is necessary in
- **Step 3c** to safeguard a uniform application of the certification scheme. In the financial industry, the well-developed supervisory structure may be sufficient to reach this aim. For the energy and transport sector, we suggest the establishment of new decision-making bodies of sectoral supervisors and cybersecurity authorities which shall be responsible for safeguarding a uniform application. Given the national nature of markets for health, water and digital infrastructure, we suggest national authorities should be responsible for the application of the cloud certification schemes.

Although a uniform application of the EU cloud security certification scheme in the public sector is unlikely, the national use by the public sector of the certification scheme would increase the relevance of the EU cloud security certification scheme and the providers adhering to it.

Table of Contents

List of Figures

List of Tables

List of Boxes

CHAPTER I: THE TECHNOLOGICAL BACKGROUND

1 Introduction: The rise of data markets

The total global amount of data created is skyrocketing. While it surpassed the amount of 40 zettabytes[1] in 2019, projections estimate it to reach 175 zettabytes by 2025 (see Figure 1).[2]

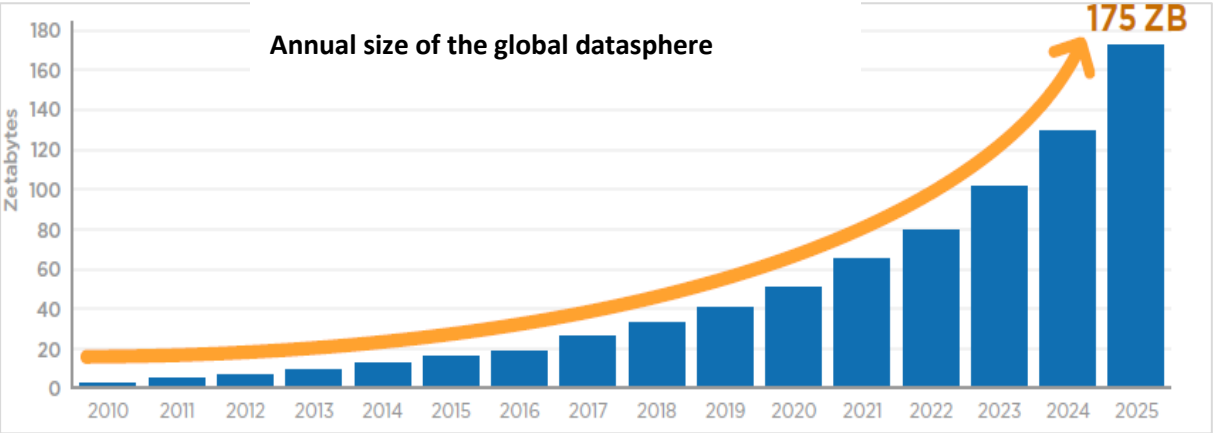

Figure 1: Annual size of the global datasphere
Source: Reinsel et al. (2018)

The value of European markets for data, defined as "the marketplaces where digital data are exchanged as products or services as a result of the elaboration of raw data"[3], are on the rise. Their value was estimated at 71,6 billion Euro in 2018.[4] The markets' value increased by more than 50% since 2013. Various projections based on three different scenarios see the European data markets grow by 2025 to levels between 93 and 141,6 billion Euro (see Figure 2). Thus, in the most positive scenario, the European data markets are about to double in size by 2025 as compared to 2018. Even in the worst scenario, an increase by 30% is expected.[5,6]

1 1 zettabyte is 1 trillion gigabyte.
2 Reinsel et al. (2018)
3 International Data Corporation (IDC) and the Lisbon Council (2019), p. 11
4 The 'value of the European data markets' is the "aggregate value of the demand of digital data without measuring the direct, indirect and induced impacts of data in the economy". It "includes imports (data products and services bought on the global digital market from suppliers not based in Europe) and excludes the exports of the European data companies". (International Data Corporation (IDC) and the Lisbon Council (2019), p. 11)
5 The 'Baseline scenario' is "characterised by a healthy growth of data innovation, a moderate concentration of power by dominant data owners with a data governance model protecting personal data rights, and an uneven but rather wide distribution of data innovation benefits in the society". The 'High Growth scenario' is "characterised by a high level of data innovation, low data power concentration, an open and transparent data governance model with high data sharing, and a wide distribution of the benefits of data innovation in the society". The 'Challenge scenario' is "characterised by a low level of data innovation, a moderate level of data power concentration due to digital markets fragmentation, and an uneven distribution of data innovation benefits in the society". (International Data Corporation (IDC) and the Lisbon Council (2019), p. 16)
6 International Data Corporation (IDC) and the Lisbon Council (2019)

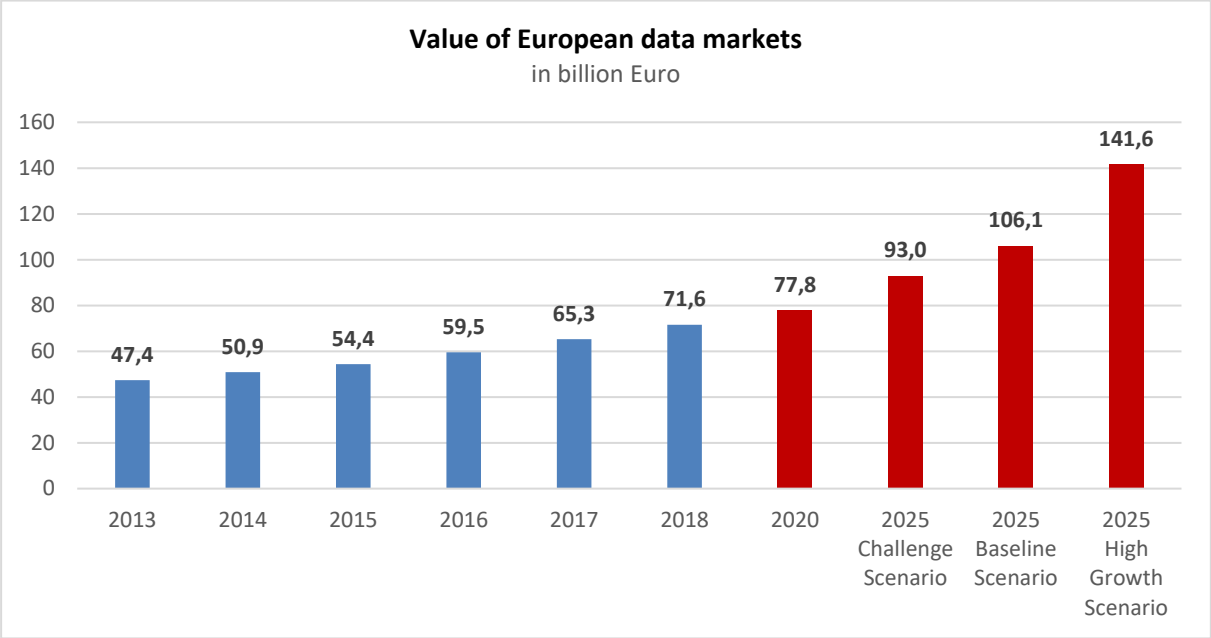

Figure 2: Value of European data markets, in billion Euro
Source: International Data Corporation (IDC) and the Lisbon Council (2019)

Even though European data markets are on the rise, they are still small in comparison to US data markets. In 2018, US data markets reached a size of 162,2 billion Euro or more than double the size of the European ones.[7] Moreover, the US markets grew year-on-year by more than 12% between 2016 and 2018, whereas EU-markets did so at a rate below 10%. Hence, the difference between US and EU markets is growing over time.

Also with regard to the amount of companies active on the supply side of data markets, the US outpaces the EU.[8] While in the US, roughly 309.000 data companies are active, the EU shows only 272.000 similar companies.[9] Although this difference seems rather small, US companies are regularly of a bigger size than the European ones.[10] Here as well, the gap between the US and the EU is growing, as the number of data companies grew between 2016 and 2018 by 6,7% in the US as compared to only 4,1% in the EU.

The total impact of the data markets on the European economy is increasing. This impact is defined as the "overall impacts of the data market on the economy as a whole". They encompass "the generation, collection, storage, processing, distribution, analysis elaboration, delivery, and exploitation of data enabled by digital technologies". [11]

When measuring total impacts of data markets, a distinction is made between direct, indirect, and induced impacts [12]:

7 As a comparison, the data markets of Japan reached a size of 29,3 billion Euro in 2018.
8 Data companies are defined as "data suppliers' organisations, whose main activity is the production and delivery of digital data-related products, services and technologies".
9 As a comparison, the amount of data companies in Japan reached 105.103 in 2018.
10 International Data Corporation (IDC) and Open Evidence (2017), p. 176
11 International Data Corporation (IDC) and the Lisbon Council (2019), p. 24.
12 International Data Corporation (IDC) and the Lisbon Council (2019), p. 24.

- Direct impacts are the initial and immediate effects generated by the data suppliers. They are measured as the revenues from data products and services sold.
- Indirect impacts are the economic activities generated along companies' supply chains by data suppliers. Indirect impacts can be backward or forward.
    - Backward indirect impacts stem from additional sales of data products and services from companies to data companies, which creates revenues.
    - Forward indirect impacts are generated through the use of data products and services by the downstream industries.
- Induced impacts are economic activities generated in the whole economy as a secondary effect.

While total impacts of data markets in the EU were just below 250 billion Euro in 2013, they increased to almost 377 billion Euro in 2018 and are expected to further increase to 1.054 billion Euro by 2025 in the most optimistic scenario (see Figure 3).[13]

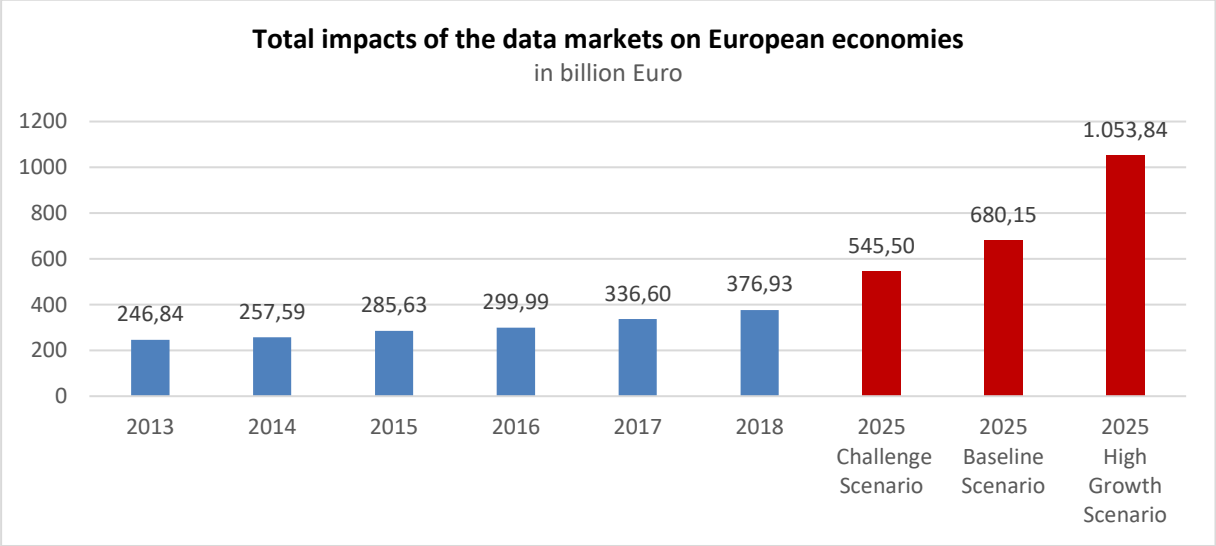

Figure 3: Total impacts of the data markets on European economies in billion Euro
Source: International Data Corporation (IDC) and the Lisbon Council (2019)

Estimates show that the European data economy's total impact accounted for 2,6% of EU GDP in 2018 as compared to 1,9% in 2013. By 2025, its relevance is expected to increase further to a level between 3,5% and 6,3% of EU GDP (see Table 1).[14]

Total impacts of data economy / GDP	2013	2014	2015	2016	2017	2018	2025 Challenge Scenario	2025 Baseline Scenario	2025 High Growth Scenario
	1,9%	1,9%	2,0%	2,2%	2,4%	2,6%	3,5%	4,2%	6,3%

Table 1: Share of total impacts of data economy / GDP in the EU
Source: International Data Corporation (IDC) and the Lisbon Council (2019)

Comparing the relative importance of the data economy in the EU and the US is not easy. US-data on forward indirect impacts and induced impacts is not available. Considering only direct and backward

13 International Data Corporation (IDC) and the Lisbon Council (2019)
14 International Data Corporation (IDC) and the Lisbon Council (2019)

indirect impacts of the data economy, it becomes clear that those impacts are much lower in Europe than in the US. This is not surprising, given that US data markets are double the size of EU markets. In 2018 those impacts accounted for 1,17% of GDP in the US and only 0,52% of GDP in the EU (see Figure 4).[15] Furthermore, in recent years, the impact of the data economy on US-GDP has increased at a faster pace than within the EU.[16,17]

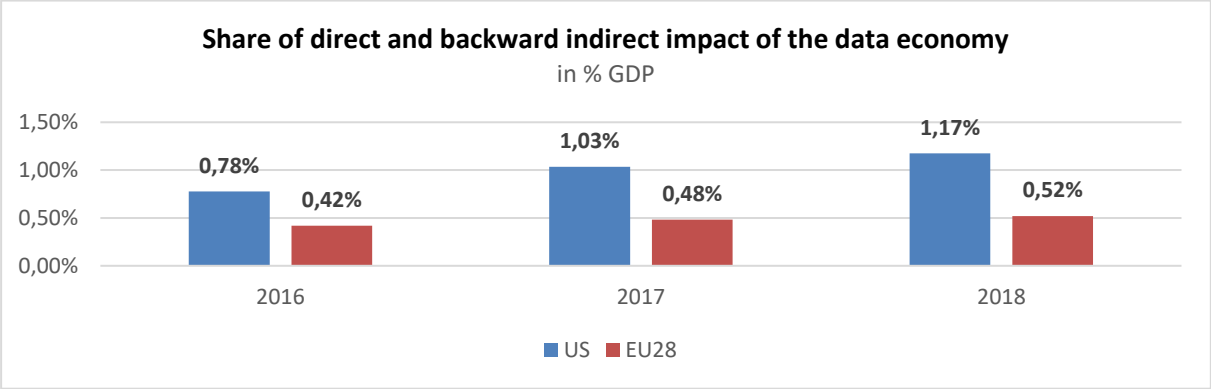

Figure 4: Direct and backward indirect impacts of the data economy in the EU and US
Source: International Data Corporation (IDC) and the Lisbon Council (2019)

2 Three global technological trends in digital markets

This chapter illustrates the most striking technological developments in digital markets in recent years and in the years to come. Firstly, a closer look is taken at the advancements in artificial intelligence, its economic impact and its current and future relevance in various world regions. Secondly, we consider the increasing use of cloud computing infrastructures and applications. Finally, we deal with the internet of things.

Importantly, it has to be mentioned that technological evolvements addressed in this chapter are intertwined and mutually dependant. Their importance today and tomorrow often depends on the technological stance of other technologies.

2.1 Artificial intelligence

The uptake of Artificial Intelligence (AI) technologies is a striking development in digital markets gaining momentum in recent years. Artificial intelligence refers to digital systems that display "intelligent" behaviour, analyse their environment and act with some degree of autonomy to achieve specific goals. AI can be purely software-based e.g. search engines, digital assistants and translation software, or be "embedded" in hardware such as robots or autonomous cars. AI facilitates economic growth and gains in efficiency across all sectors, such as better health care, e.g. by more accurate and faster medical diagnoses, a safer transport sector due to autonomous vehicles, a more sustainable

15 As a comparison, the direct and backward indirect impacts of the data economy in Japan reached 1,05% of GDP in 2018.
16 International Data Corporation (IDC) and the Lisbon Council (2019)
17 As a comparison, the impacts in Japan increased by 9,79% between 2018 and 2017.

economy through the reduction in energy consumption and a lower use of pesticides in agriculture and more efficient production processes through robots taking on repetitive and dangerous tasks.[18]

The global artificial intelligence market value stands at 10,6 billion US dollars in 2019 and is estimated to increase to 34,6 billion US dollars by 2021.[19] AI could "contribute up to 15,7 trillion US dollar to the global economy in 2030".[20] This corresponds to an increase in worldwide GDP of 14%. China and North America are expected to profit the most from AI related innovations, technologies and productivity gains (7 vs. 3,7 trillion US dollar) while impact in Europe is estimated to reach 2,5 trillion US dollar (see Figure 5).[21] Thus, China and Northern America will together reach 68% of the total global impact, while Europe's global share only sums to 16%.

AI may produce productivity gains as well as consumption-side effects. While the former include e.g. the automation of routine tasks, the latter encompass effects stemming from higher quality and more personalised products and services. Roughly, 42% of the estimated economic impact of the 15,7 trillion US dollar are expected to relate to productivity gains, while 58% comes from consumption-side effects.[22]

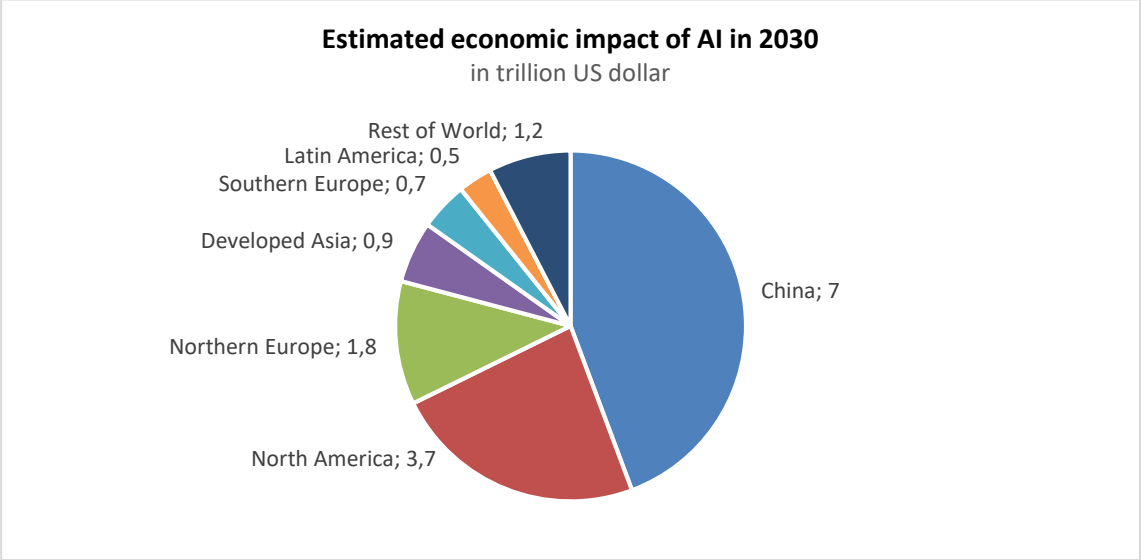

Figure 5: Economic impact of AI in 2030
Source: PWC (2017)

Accenture estimates that AI could almost double the annual growth rates of real gross value added by 2035.[23] For a dedicated group of countries, which include the US, Japan and several European countries, they predict a growth with AI of 3,2% on average compared to 1,7% without AI. The highest AI-related additional growth is expected for the US (2%-points), Finland (2%-points), Sweden (1,9%-points) and Japan (1,9%-points). Germany reaches an 1,6%-point increase (see Figure 6).

18 Artificial Intelligence for Europe – Pillar 1: Investment in AI, cepPolicyBrief No. 2019-10, cep
19 GosReports, http://www.gosreports.com/global-artificial-intelligence-market-research-report-2017/
20 PwC (2017)
21 PwC (2017)
22 Id.
23 Accenture (2017)

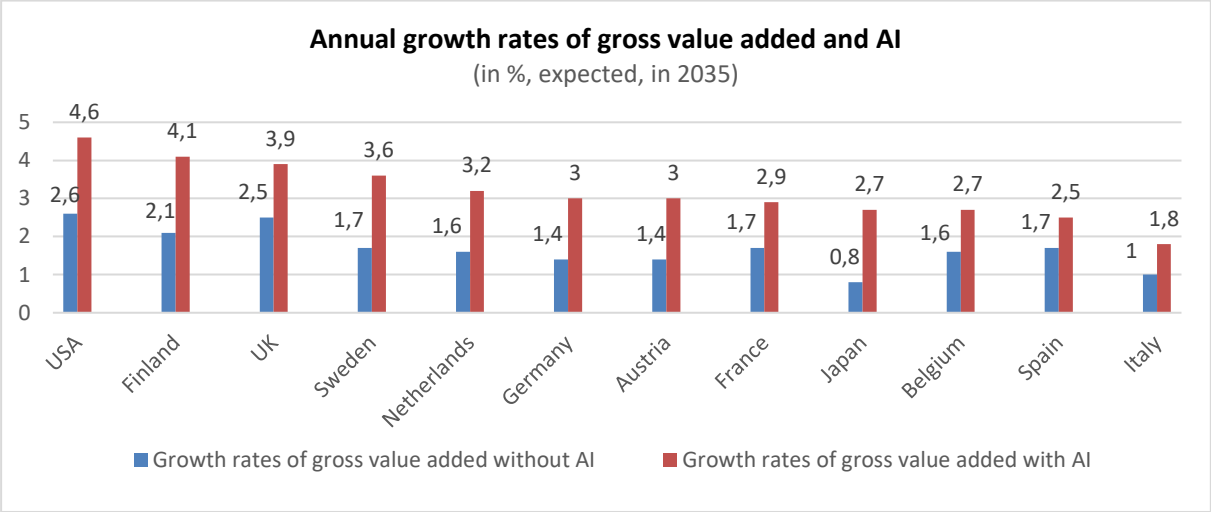

Figure 6: Annual growth rates of gross value added with and without artificial intelligence
Source: Accenture (2017)

The growing importance of AI technologies can also be seen in patent statistics. According to OECD-data, annual growth rates of AI-related patents significantly outpace the growth rates of total patents in recent years. While AI patent growth has been 6,6% on average between 2010 and 2015, total patent growth reached only 3,5% (see Figure 7).

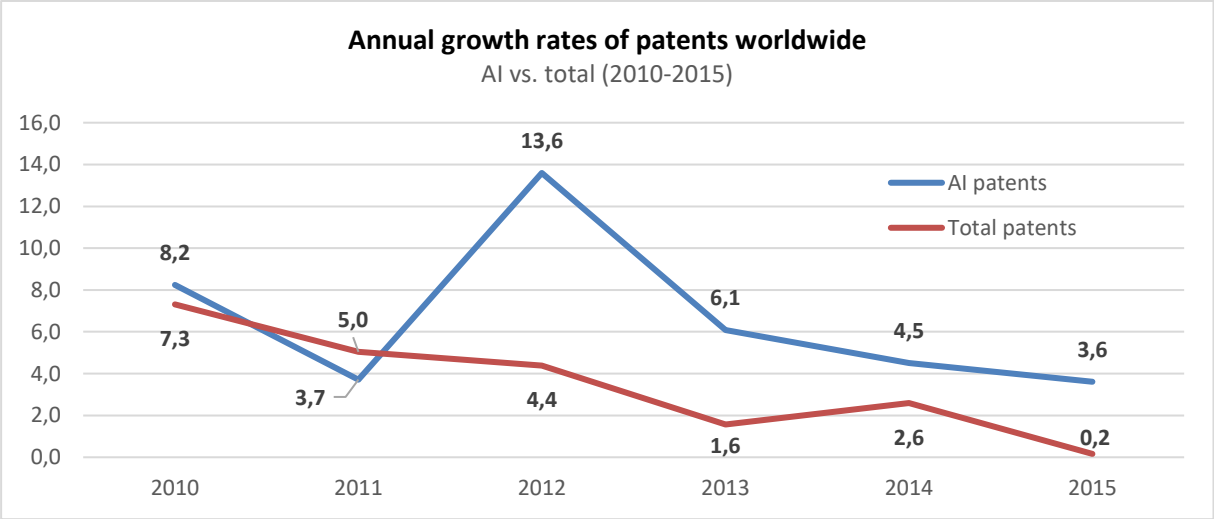

Figure 7: Annual growth rates of AI patents vs. total patents (2010-2015)
Source: OECD (2017)

In the period 2010-2015, Japan (27,9%), Korea (17,5%) and the US (17,2%) accounted for the highest share of AI related patents. The EU28 ranked fourth with a share of 11,9%, before China (10,4%). The relative share of importance of Japan, the US and the EU significantly fell as compared to the period from 2000-2005. Korea, China and Taiwan increased their stake in the AI markets remarkably (see Figure 8).

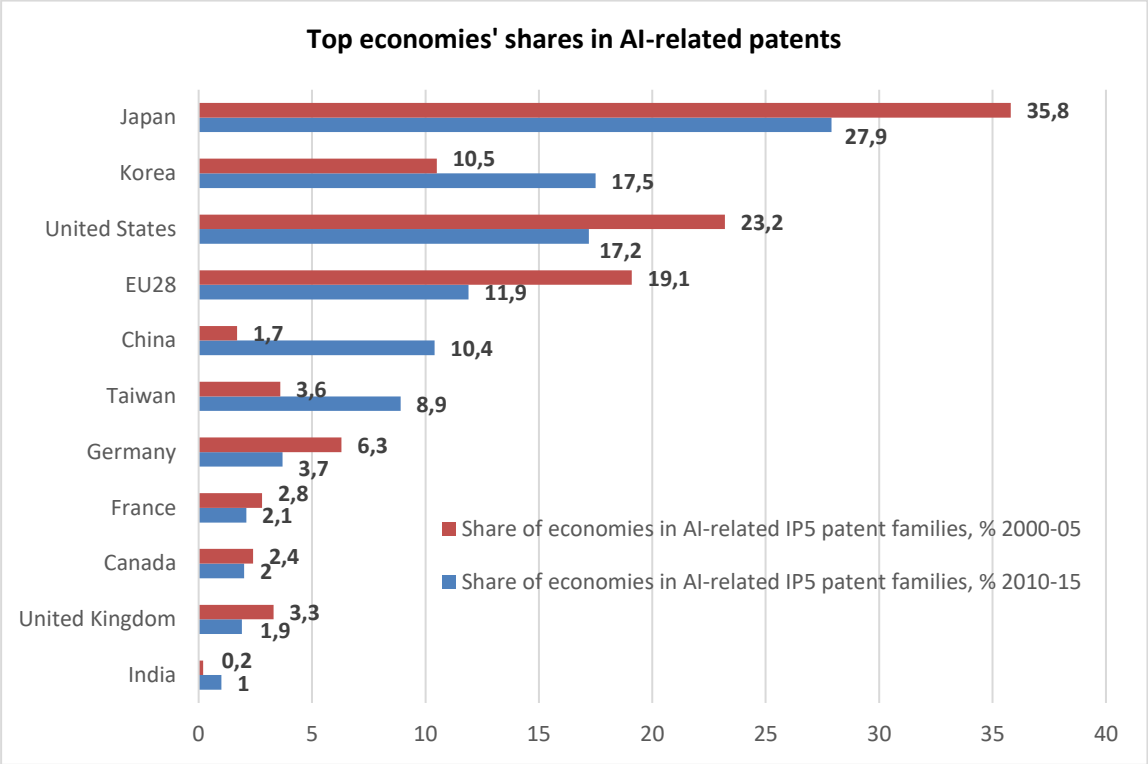

Figure 8: Top economies' shares in AI-related patents, %, 2000-2005 and 2010-2015
Source: OECD (2017)

From 2011 to mid-2018, the US, China and the EU together accounted for more than 93% of AI-related private equity investments globally. Total investments amounted to more than 50 billion US dollar. In 2017, the EU accounted for 8% of AI-related private equity investments, up from only 1% in 2011.[24] With more than two thirds of AI-related investments, the US attracts most of the investments since 2011. While China was lagging behind the EU until 2016, it experienced a tremendous increase in investments since then. While China accounted for only 3% of total investments in 2015, in 2017 start-ups already attracted 36% of investments. Consequently, the EU only ranks third since 2016 (see Figure 9).[25]

[24] Between 2011 and mid-2018 the United Kingdom received 55% of the EU total investments. Germany and France only accounted for 14% respectively 13%. Consequently, in case of a Brexit, the global share of AI private equity investments of the EU is likely to shrink significantly.

[25] OECD (2018)

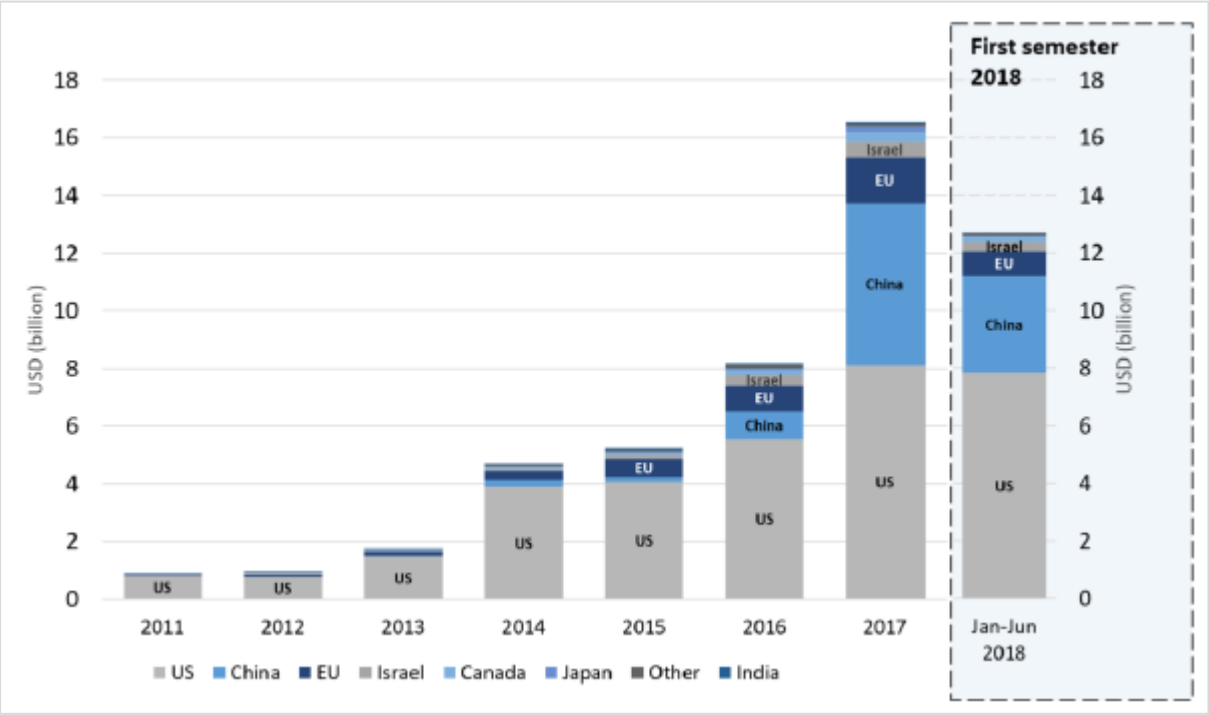

Figure 9: Private equity investments in AI start-ups, by start-up location
Source: OECD (2018)

2.2 Cloud computing

Cloud computing is defined by the National Institute of Standards and Technology (NIST)[26] as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction".[27] Clouds basically allow to store and access data and programs on or via the Internet.

There are three main cloud computing service models:

- Infrastructure as a Service (IaaS) is the basic type of cloud computing model, where users can access computing resources – e.g. servers, storage – on the cloud.
- Platform as a Service (PaaS) provides a platform for users to develop, manage and deliver applications.
- Software as a Service (SaaS) allows users to access a cloud-based software on a rented basis, where they can use applications without having to install them on their local devices.

Within the European Union, the share of enterprises using could services rose by 37% since 2014. In 2018, 26% of enterprises used cloud services (2014: 19%). Only 25% of European small and medium enterprises (SMEs) use cloud services, whereas the use of clouds is much more widespread amongst larger enterprises (56%).[28] Whereas this trend can be observed in all Member States, significant differences persist. The use of corporate cloud computing services is much more widespread in Nordic

[26] The NIST is part of the Department of Commerce of the United States. It is in charge of innovation and industrial competitiveness. Its definition of the cloud computing is the most common one.
[27] Mell P. and Grance T. (2011)
[28] Cloud computing - statistics on the use by enterprises, Statistics Explained, December 2018.

countries (65% in Finland, around 55% in Sweden and Denmark), compared to Germany, Italy and France (about 20%) (see Figure 10).

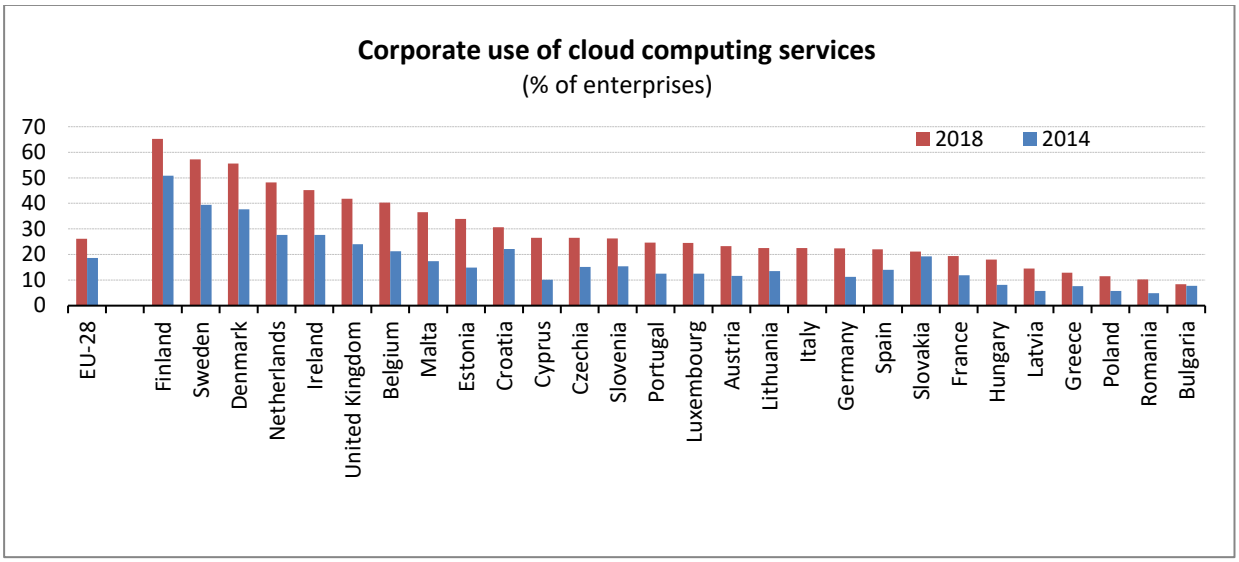

Figure 10: Use of cloud computing services, 2014 and 2018, (% of enterprises)
Source: Eurostat

Clouds can be deployed as public or private clouds. Private clouds are designed for a single user/company and are delivered from servers of a cloud provider reserved to the specific user. On the opposite, in public clouds, resources are shared by multiple users and cloud services are delivered from shared servers of the cloud provider. Clouds can also be hybrid, i.e. a private cloud may be combined with the use of public cloud services. A majority of cloud workloads and compute instances – i.e. a set of computer resources running a specific application or providing computing services – are in the public cloud (58% in 2016) compared to the private cloud (42% in 2016). This trend is expected to continue. The number of public cloud workloads and compute instances is estimated to grow by 28% on a yearly basis to reach 73% of the overall cloud workloads in 2021, while private cloud workloads and compute instances are expected to grow at 11% annually and represent 27% of the overall cloud workloads in 2021 (see Figure 11).

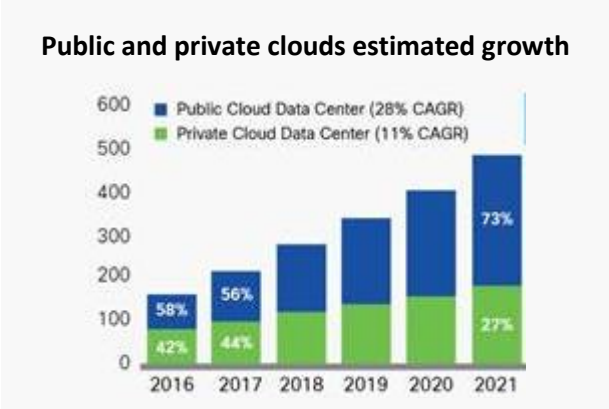

Figure 11: Public vs. private clouds
Source: Cisco (2018)

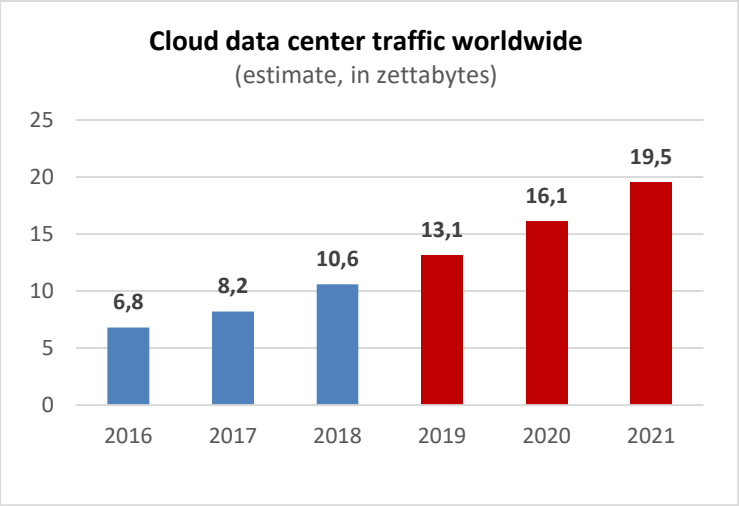

Figure 12: Cloud data center traffic in zettabytes

Source: Cisco, Global Cloud Index, 2016-2021

The use of cloud services is expected to grow substantially by 2021. The estimated amount of traffic entering and exiting cloud data centres in 2016 was 6,8 zettabytes and it is expected to reach 19,5 zettabytes by 2021 (see Figure 12). In 2018, data traffic within cloud-based data centres was already 11 times the size of traffic within traditional data centres (10,6 zettabytes vs. 1,046 zettabytes).[29]

Estimates on the future number of cloud data centre workloads and compute instances shed insight on the growth of the cloud economy and its geographical centres. North America and Asia Pacific show the highest number of cloud workloads and compute instances with respectively 81 and 61 million in 2016, followed by the Western Europe region with 39 million. This is not expected to change substantially. Asia Pacific (201 million) and North America (192 million) are set to reach higher numbers than Europe (97 million) (see Figure 13).[30]

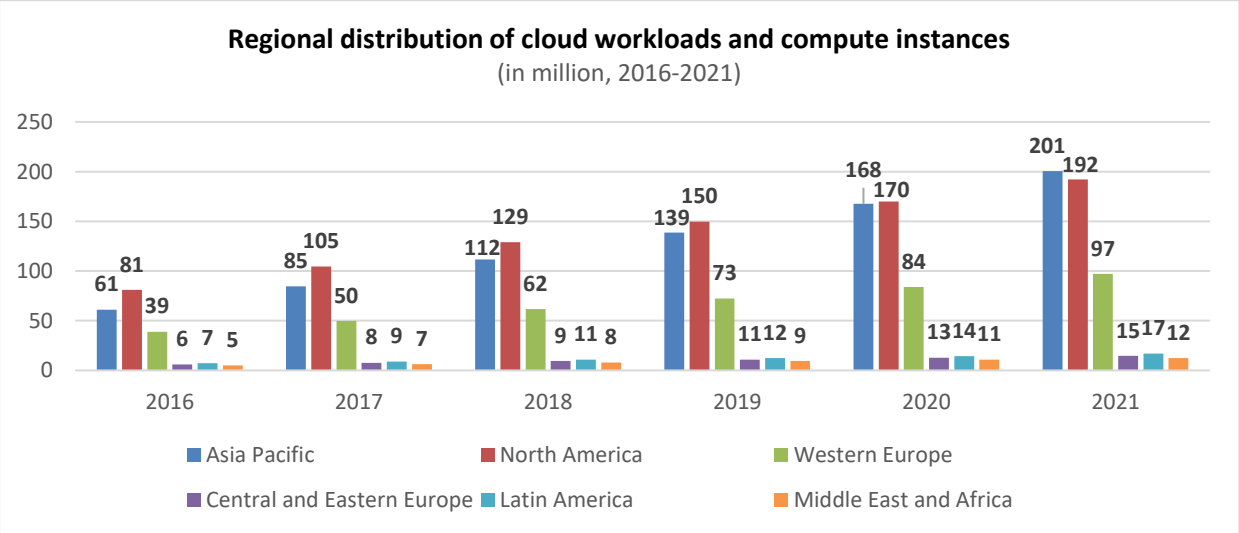

Figure 13: Regional distribution of cloud workloads and compute instances in million

Source: Cisco Global Cloud Index, 2016-2021

29 Roland Berger and Internet Economy Foundation (IEF) (2019), p. 15.

30 Figure 13 does not account for the aspect that companies located in one region may use a lot of cloud workloads and compute instances in other regions. For instance, Western Europe companies may use a lot of facilities in North America increasing the amount of cloud workloads and compute instances there, or vice versa.

Business models related to cloud computing are gaining importance. Public cloud application services (SaaS) generate the greatest revenue today (94,8 billion US dollar in 2019) and will be so also in 2022 (143,7 billion US dollar).[31] However, public cloud system infrastructure services (IaaS) are estimated to catch up in the years to come (see Figure 14).[32]

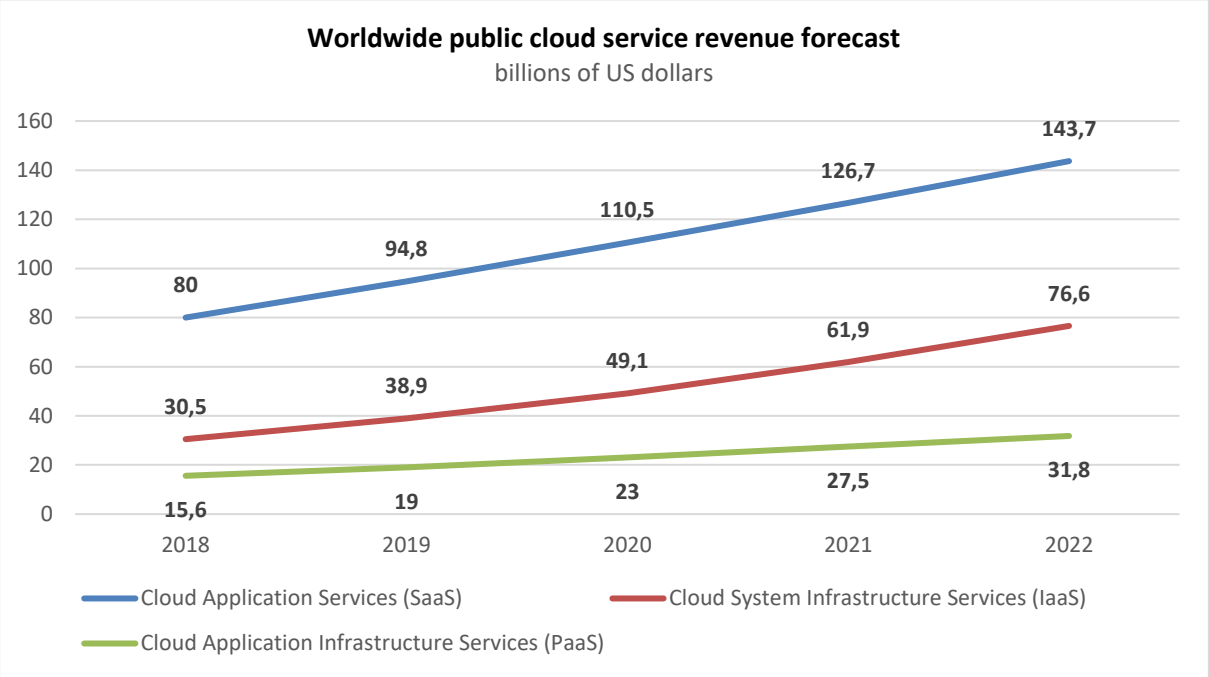

Figure 14: Worldwide public cloud service revenue in billions of US dollars
Source: Gartner

Amazon is the dominant cloud computing player in the 4th quarter of 2018, followed by Microsoft, Google, Alibaba and IBM. These five companies, often referred to as the "hyperscalers" account for 66% or 15 billion US dollar of the turnover made in cloud computing. Other companies generate 7,7 billion US dollars or 34% of the whole market. In the 4th quarter of 2017 the share of the hyperscalers stood at 61%[33] (see Figure 15).

31 https://www.gartner.com/en/newsroom/press-releases/2019-04-02-gartner-forecasts-worldwide-public-cloud-revenue-to-g

32 This figure only shows developments in the market for 'public clouds' and not for 'private clouds'.

33 https://www.canalys.com/static/press_release/2019/pr20190204.pdf

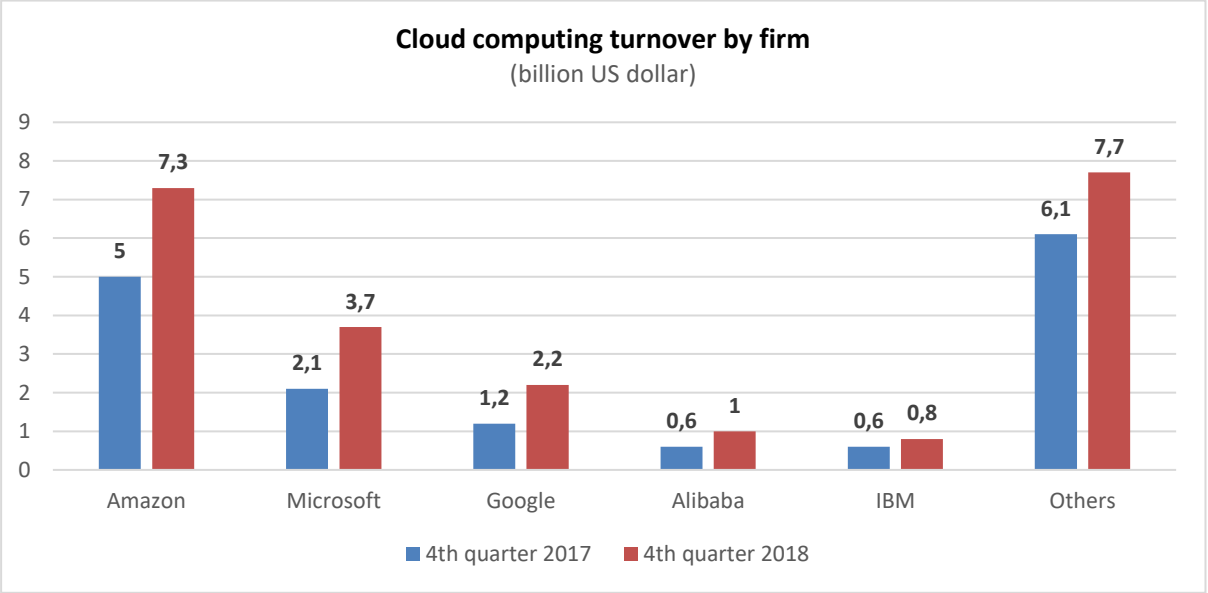

Figure 15: Cloud computing revenues by firm
Canalys Cloud Channels Analysis, February 2019

Concentration in the sub-cloud market differs. Concentration levels are highest in the IaaS and the PaaS segments, where the three main players account for 63% (IaaS) respectively 58% of the market in 2018. In contrast to those two segments, the SaaS segment is still quite fragmented. The biggest market participants (Salesforce, SAP and Oracle) account for 25% of the whole SaaS market (see Table 2).

Three main players in cloud computing sectors worldwide (Market share in %)	1st	2nd	3rd	Market share top 3 2018
Infrastructure as a service (IaaS)	Amazon (42%)	Microsoft (15%)	IBM (7%)	**63%**
Platform as a service (PaaS)	Amazon (32%)	Microsoft (16%)	Salesforce (10%)	**58%**
Software as a service (SaaS)	Salesforce (12%)	SAP (7%)	Oracle (5%)	**25%**

Table 2: Market Concentration in the cloud computing market worldwide
Source: Confidential with data from Gartner

2.3 Internet of Things

The Internet of Things (IoT) is defined by the International Telecommunication Union[34] as a "global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies." The IoT allows to connect physical – e.g. a watch or a lamp – or virtual objects to other objects and to the Internet, thus creating smart environments.

The IoT is already used by businesses in various cases and can bring a lot of advantages, notably efficiency gains. For example, smart metering allows

[34] The ITU is an agency of the United Nations specialised in the field of telecommunications, information and communication technologies.

- energy companies to monitor consumers' electricity or water consumption and adjust the prices to the time of day and the seasons;
- utilities to optimise energy distribution, reduce operational expenses linked to manual operations and improve forecasting of power-consumption;
- predictive maintenance through sensors, cameras and data analytics which can determine when an equipment will fail and inform the company managers. Companies can therefore better plan maintenance and reduce costs.

The IoT is a fast-growing technological area, seen as one of the next major breakthroughs in the development of digital technologies.[35] The overall worldwide spending on the IoT is expected to reach 745 billion US Dollar by the end of 2019, which represents an increase of 15,4% compared to the 646 billion US Dollar spent in 2018.[36] The number of IoT devices in-use worldwide is also growing. From 15 billion devices installed in 2015 it is estimated to double by 2020 and reach 75 billion devices in 2025 (see Figure 16).

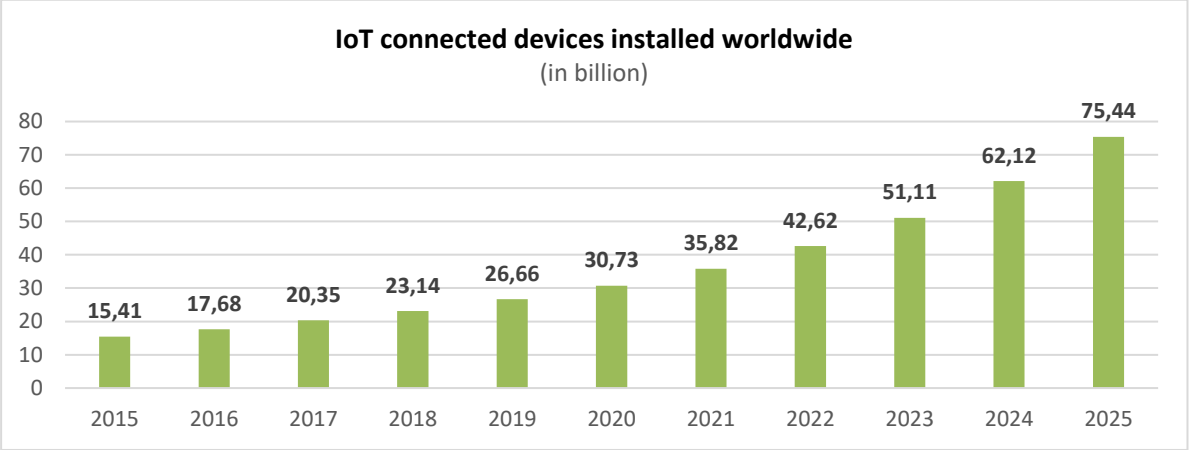

Figure 16: Number of IoT connected devices worldwide 2015-2025
Source: Statista

3 The role of platforms in digital markets

Platforms are a characteristic feature of the digital economy. Platforms are neither new nor exclusively relevant to the digital economy. They play an important role also in the analogue economy. However, as platforms are ubiquitous in the digital economy, a thorough understanding their functioning is key to identifying the policy challenges ahead. In the following, we briefly explain some of the essential characteristics of platforms.

3.1 Two- and multi-sided platforms

Platforms mostly act as intermediaries to connect users – both private and professional. Therefore, one characteristic of platforms is that they help users "to get together in a way that generates value for these"[37] users. Platform owners may charge users for this service.

35 The Joint Institute for Innovation Policy et al. (2019), p. 11.
36 IDC, Presse release from 03 January 2019, available at: https://www.idc.com/getdoc.jsp?containerId=prUS44596319
37 Evans D. (2009)

If all platform users belong to the same group, in other words, when platform users are homogenous, the platform is considered to be one-sided.[38] One example of this is a social network without advertising. If the platform users belong to different groups e.g. consumers, retailers or advertisers it is a two- or multi-sided platform. One example of this is a social network with advertising.

Most platforms in the digital economy industry are at least two-sided.[39] According to the OECD, a two- or multi-sided platform is characterised by three elements:[40]

- There are at least two heterogeneous user groups who want to interact "and who rely on the platform to intermediate transaction between them."[41]
- There exist indirect externalities (also called network effects) across the user groups. Indirect network effects mean that the benefit of a user at one side of the platform "increases with the number of users on the other side."[42]
- The added value the platform generates depends on the price level and the price structure. The price level is the price charged per transaction on both sides of the platform.[43] The price structure is the allocation of the price level between both groups.

The first element – the existence of two different user groups – is straight-forward at first sight. However, it might be difficult to detect the platform, for example in the case of operating systems. An operating system is a platform that connects application developers and application users as it facilitates the developing of an app. The same may go for cloud service providers.

The second element – the indirect externalities – explains the high concentration in of platforms in the digital economy. Due to network effects, there often is room for a few platforms only. The cost structure of some platforms – high fixed and low marginal costs – aggravates this problem. Examples of this are the low number of relevant players in the markets for mobile phone operating systems or hyper cloud service providers.

The third element – the influence of price structure – has its roots in the fact that the groups that use a specific platform often differ in their price sensitivity. As a platform needs both sides of a platform in order to be successful, the platform operator attracts the group with the greater price sensitivity by charging this group less. In some cases, this price might even be zero, meaning the group with the lower price sensitivity subsidises the group with the greater price sensitivity.

3.2 Platforms and market concentration

Platforms regularly show a high market concentration with one platform having a very high market share (e.g. Google, Facebook, Amazon in the B2C-Sector or AWS, Google and Microsoft in the B2B-Hyper Cloud Market). Of course, platform owners have often developed innovative products or services, making the platform worth using for all market sides. Nevertheless, there are three explanations for this platform concentration trend. Separately or combined, they can form serious obstacles

38 Monopolkommission (2014), para. 300.
39 Evans D. (2009), p. *23.*
40 OECD (2011), p. 3
41 Id.
42 Id.
43 Evans D. (2009)*, p. 28.*

for potential competitors to existing platforms and hence cause serious competition problems.

- Network effects: Additional users on one market side attract additional users on the other market side. This reinforces attractiveness to users on the first market side and so on. These effects are particularly relevant for cloud service, sales platforms and social networks.

- High fixed costs: Building a platform may cause high fixed costs, while variable costs of running a platform are mostly low. This leads to high market entry barriers for competitors. The platform may hence become a natural monopoly as it is not worthwhile to duplicate it.

- Lock-in effect: Lock-in effects exist if it is costly for users of a platform to switch to another platform. This may be the case for social networks, sales platforms or cloud service platforms.

While these forces foster platform concentration, there are other forces that have the opposite effect:

- Multi-Homing: Multi-homing means the simultaneous use by users of different platforms. This may reduce concentration tendencies only when *all* user groups are able to conduct multi-homing. If only one group, e.g. consumers, have the possibility to use more than one platform at the same time, while the other user group (e.g. retailers) cannot, the consumers have no incentive to switch to another platform. In practice, these hurdles for retailers can arise from limits to transferring positive user ratings to new platforms.[44] In the case of mobile operating systems, especially users face high costs of multi-homing. In B2B-contexts, corporate users may be more willing to use multi-homing, e.g. in the hyper cloud market.

- Product Differentiation: Platforms may differentiate the quality of their products, depending on the differences amongst users' preferences. Product differentiation may be horizontal (different products in one given quality) or vertical (one product in different qualities). Product differentiation reduces search costs for platform users and increases the possibility to find the right match. Therefore, platform concentration may be reduced.

- Innovation: Innovation can mitigate concentration of platforms.[45] The digital economy is a dynamic and innovative industry. Its markets are characterised by short product lifecycles and regularly changing consumer preferences. New platforms picking up new products and services increase competition pressure.

44 Monopolkommission (2014), paragraph 380.
45 Monopolkommission (2014), paragraph 51.

3.3 Market concentration in B2C vs. B2B

In general, the B2B market shows less effects supporting a market concentration than the B2C market. To the contrary, market participants in the B2B space usually avoid dependencies on a single source, i.e. do not rely on it without sourcing otherwise in parallel.

With respect to the characteristics, B2B platforms differ somewhat when compared to B2C platforms.

First, network effects of B2B platforms tend to be smaller than of B2C platforms as the potential network is usually smaller. Thus, market concentration is less pronounced in B2B markets. On the contrary, it is noticeable that a lot of different platforms exist and many firms still offer their own platforms and do not use those of third parties.

Second, the contracts between the users and the B2B platforms are more individualised.

Third, the fact that many companies do not rely on platforms of others, means that economies of scale caused by high fixed and low variable costs are not fully exploited. Or put differently: "*You can't compare a heavily segmented, indeed fragmented and highly specific industry such as mechanical engineering with the big, wide world of end-customer business that sells books, overnight stays and passenger transport. Nor […] do platforms command the same importance in this line. That is probably the reason why the market volume addressed by platforms in the B2B environment will indeed never reach B2C-like dimension"*[46].

Fourth, the risk of congested platforms is higher for B2B platforms (at least in the manufacturing sectors) as they more often rely on physical products instead of digital ones in case of B2C platforms. This limits their growth as physical products are subject to wear.

Fifth, as incentives for differentiation in the B2B market are strong, the risk for monopolistic B2B platform scenarios is smaller. For instance, a lot of sector specific B2B platforms do coexist in the manufacturing industry.

And fifth, whether multi-homing is easier in the B2B context cannot be judged as of today, but a lot of companies seem to be active on many platforms.[47,48]

46 Platform Economics in Mechanical Engineering, Challenges – opportunities – courses of action, VDMA, May 2018
47 Bundesministerium für Wirtschaft und Energie (BMWi) (2019a)
48 Bundesministerium für Wirtschaft und Energie (BMWi) (2019b)

CHAPTER II: PRIORITY 1 – TOWARDS A SINGLE MARKET FOR DATA

This chapter sets out nine recommendations on how to foster the development of European data markets. The need for a single market for data is obvious. The success of digital business models depends to a considerable extent on the ability of providers to scale and rapidly reach a critical mass of customers and to access a large amount of data for the development of new digital services. Providers in the US and China benefit from large and homogenous data markets, which provide them with a competitive edge. Hence, the creation of a fully functioning single market for data should be a priority for the European Commission.

In Part 1, we first delineate different types of data and briefly set out some relevant aspects of their regulatory treatment in the EU. Explaining some of the most relevant characteristics of data, we then set out in Part 2 why pooling and sharing data is economically useful and the establishment of secondary data markets would be of great benefit. Part 3 offers an overview of some of the most relevant bottlenecks to trading and sharing data. In Part 4, we offer nine recommendations aiming at fostering the pooling and sharing of personal, business and public data.

1 Data: Definition and regulatory treatment in the EU

1.1 Data vs information

Data is a buzzword without commonly accepted definition.[49] Data can be characters, character strings, indications, (numerical) values or findings and can be obtained e.g. by measurement or observation. Data is hence very heterogenous and may be very different as concerns its

- **origin**: data may be personal, non-personal, mixed or public sector data;
- **production manner**: data may result from private digital behaviour, from mandatory reporting to authorities, from corporate processes or may be machine-generated; it may be measured or observed;
- **quality**: data may be standardised and comparable or very unclean;
- **use:** data may serve as an input to very different services aiming at both retail and corporate users.

As the different uses of data indicate, it is important to differentiate between data and information. In fact, data is a factor of production in producing information.[50,51] For the data economy, not data as such is important, but the information that can be derived out of the data. The expression 'information good' is often used to describe this, indicating the information that can be depicted from data as the valuable asset.[52]

In the following, we distinguish between personal, public and non-personal data.

---

49 An article by Zins identified 130 definitions of data, information, and knowledge in 2007 [Zins (2007)].

50 Jones and Tonetti (2018)

51 Fröhlich-Bleuler (2017)

52 For reasons of simplification, in the remainder of the paper, we will generally stick to the term 'data' instead of 'information good'.

1.2 Personal data and the General Data Protection Regulation

When processing data of EU data subjects, market actors need to comply with the personal data protection framework. This includes human rights law, which restricts access to personal data. Notably, while Article 7 of the Charter of Fundamental Rights of the European Union ("the Charter") qualifies privacy as a fundamental right, Article 8 of the Charter is of more direct relevance, as it specifically establishes that everyone has the right to the protection of personal data concerning him or her.

Under Article 8, personal data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Furthermore, everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. Compliance with these rules must be subject to control by an independent authority.

The right to the protection of personal data is also established by Article 16 (1) TFEU.[53] Processing of personal data is now also comprehensively regulated under EU secondary law, i.e. by the General Data Protection Regulation ("GDPR").[54]

1.2.1 Fundamentals of the General Data Protection Regulation

The GDPR lays down rules concerning (i) the protection of natural persons with regard to the processing of personal data and (ii) the free movement of such data across the internal market.[55]

It replaces the Data Protection Directive[56] of 1995 with the view of, on the one hand, making the legal framework fit for the new challenges posed by technological developments and, on the other, achieving a greater level of harmonisation than the Directive.[57] The 2016 Regulation also codifies the relevant case law that the CJEU has built up in the course of the previous decade.[58]

As to the fundamental traits of the new regulatory regime, they can be summarised as follows:

- establishment of new rights and rules allowing the individual to keep control of his/her data;

---

53 The insertion of Article 16 TFEU within the Lisbon Treaty was crucial because for the first time it established a legal basis granting the EU the competence to legislate on data protection matters. While EU data protection rules were initially based on the internal market legal basis and, therefore, justified by the specific need to smoothen the free movement of data within the EU, "*Article 16 of the TFEU now provides an independent legal basis for a modern, comprehensive approach to data protection, which covers all matters of EU competence, including police and judicial cooperation in criminal matters*" (European Union Agency for Fundamental Rights and Council of Europe (2018), pp. 28-29).

54 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (O.J. 2016, L 281/31).

55 Article 1 GDPR

56 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (O.J. 1995, L 119/1).

57 "The objectives and principles of Directive 95/46/EC remain sound, but it has not prevented fragmentation in the implementation of data protection across the Union, legal uncertainty or a widespread public perception that there are significant risks to the protection of natural persons, in particular with regard to online activity. Differences in the level of protection of the rights and freedoms of natural persons, in particular the right to the protection of personal data, with regard to the processing of personal data in the Member States may prevent the free flow of personal data throughout the Union. Those differences may therefore constitute an obstacle to the pursuit of economic activities at the level of the Union, distort competition and impede authorities in the discharge of their responsibilities under Union law. Such a difference in levels of protection is due to the existence of differences in the implementation and application of Directive 95/46/EC" (GDPR, Recital n. 9).

58 Korff D., Georges M. (2019), pp. 102 ff

- accountability for compliance with the Regulation lying on the subject who takes the decision as to if, why and how data is to be processed, i.e. the controller;
- supervision of controllers and processors by the national Data Protection Authorities ("DPAs");
- obligation for the Member States to introduce effective remedies for the infringements of the data protection regime and the damage eventually caused by them;
- a dissuasive sanction system (of higher fines).

1.2.2 The key to interpreting the GDPR: the fundamental right to personal data protection

The provisions of the GDPR govern an activity, i.e. processing, which affects the fundamental right to personal data protection and the right to respect for private life. This means that such provisions must necessarily be interpreted in the light of the Charter of Fundamental Rights of the European Union (the Charter), Article 8 of which ensures the right to the protection of personal data.[59]

Besides, the GDPR expressly acknowledges the relevance of the fundamental right to personal data protection[60] and embodies it in most of its core principles. This is particularly the case for the *principle of data minimisation*, according to which, in order to minimise the risks to the right to personal data protection, processing must be "adequate, relevant and limited to what is necessary".[61] The same goes for the *principle of storage limitation*, i.e. the principle requiring personal data to be kept in a form that limits in time the identifiability of the data subject to the minimum extent necessary for the purposes of processing.[62]

The relevance of the Charter for interpreting the GDPR bears two important consequences. First, Article 52 (1) of the Charter applies. According to this provision, a limitation of the right to data protection is only legitimate when necessary and genuinely devoted to meet objectives of general interest recognised by the Union, or to protect the rights and freedoms of others.[63] Accordingly, in so far as the GDPR establishes restrictions of the right to protection of personal data (e.g. the ones provided for by Article 23 GDPR), it needs to be interpreted strictly. By the same token, limitations of this fundamental right are only legitimate in so far as they rely on an accurate balancing of the interests at stake, so as to minimise the sacrifice of the fundamental right to personal data protection while emphasizing the necessity to balance it with other fundamental rights[64].

Secondly, Article 52 (2) of the Charter is also relevant for the interpretation of the GDPR. Article 52 (2) prescribes that, in so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), the meaning and scope of those rights shall be the same as those laid down by the said Convention. This means, most notably, that the case law of the European Court of Human Rights (ECtHR) is relevant for the interpretation of the Charter.

This requires a clarification.

---

59 Judgment of 6 October 2015, Schrems, C-362/14, EU:C:2015:650, para. 38; judgement of 17 July 2014, YS and Others, C-141/12, EU:C:2014:2081, para. 54.

60 See Considerandum n. 4 GDPR.

61 Article 5(1)(c) GDPR

62 Article 5(1)(e) GDPR

63 Judgement of 9 November 2010, Volker und Markus Schecke and Eifert, C-92/09, EU:C:2010:662, para. 65.

64 Recital 4 GDPR

Admittedly, Article 8 of the Charter does not directly correspond to any article in the ECHR: while Article 8 (2) ECHR seems to ensure, *inter alia*, the right to the protection of personal data by establishing a broader right to respect for private life[65], it does not, unlike Article 8 of the Charter, confer any specific right to the data subject, it lacks any reference to the legitimate grounds for processing and to the supervision by an independent authority. Besides, Article 8 ECHR only deals with interferences by public authorities, whereas Article 8 of the Charter also mentions the case of limitation of the fundamental right to personal data protection due to the existence of competing rights.

One circumstance suggests nevertheless that Article 8 (2) ECHR and the related case law of the ECtHR are relevant for interpreting the right to data protection under EU law: according to the Explanations relating to the Charter of Fundamental Rights, Article 8 of the Charter was based on Article 8 ECHR and on the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data, which has been ratified by all the Member States.[66] This link, which "ensures the existence of mutual inspiration between the CJEU and the ECtHR on matters related to data protection"[67], is recognised by the case law of the CJEU.[68]

1.2.3 Material scope

Under its Article 2, the GDPR governs *any* processing operation of *any* personal data. The broad definition offered by the GDPR of the terms "personal data" and "processing" makes the Regulation applicable in a wide variety of cases.

More specifically, "processing" means "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means".[69]

As to the term "personal data", it covers "any information relating to an identified or identifiable natural person", i.e. a "data subject". The relationship between the data and the data subject can be established "by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person"[70].

In this respect, it should be underlined that the approach taken by the legislator as to when a natural person can be qualified as "identifiable" is of particular relevance for understanding the breadth of the notion of "personal data". To determine whether a natural person is identifiable, account should be taken of "*all the means reasonably likely to be used* […] *either by the controller or by another per-*

---

65 Article 8, "Right to respect for private and family life"- 1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

66 Explanations relating to the European Charter of Fundamental Rights (2007/C 303/02), Art. 8.

67 European Union Agency for Fundamental Rights and Council of Europe (2018), p. 52

68 See, *inter alia*, judgement of 9 November 2010, Volker und Markus Schecke and Eifert, C-92/09, EU:C:2010:662, para. 59. For an express recognition of such link, see the opinion of A.G. Villalón in Digital Rights Ireland and Seitlinger and Others, C-293/12, EU:C:2013:845, para. 62.f.

69 Among relevant operations, the GDPR mentions collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction [Article 4(1)(2) GDPR].

70 Article 4(1)(1) GDPR

son to identify the natural person directly or indirectly"[71, 72]. Also, "[t]*o ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments*"[73].

Data that qualifies as personal can still be subject to *anonymisation*, i.e. "a technique applied to personal data in order to achieve irreversible de-identification".[74] In this case they are de-personalised and their processing falls out of the scope of the GDPR.[75] However, one must keep in mind that the boundaries between personal and non-personal data in the Big Data economy with data-aggregating processes and techniques are fluid. The debate as to when data can be said to be legally anonymised is far from over.[76]

1.2.4 Data localisation requirements

The EU General Data Protection Regulation provides the framework for the free flow of personal data within the EU so that local storage or local processing of personal data becomes obsolete. For international transfers of personal data, the GDPR requires additional safeguards to ensure that the level of protection for data subjects travels with the data.

The GDPR allows for national data localisation requirements as long as those are not connected "with the protection of natural persons with regard to the processing of personal data".[77]

At the same time, the GDPR – and its restrictions for data localisation requirements – do not (fully) apply in a number of cases:

- Personal data processing may fall out of the scope of the GDPR. While the broad definition of "personal data"[78] and "processing"[79] makes the scope of application of the GDPR extremely large, Article 2 para. 2 GDPR lists cases where the GDPR does not apply, i.e.:
    a. in the course of an activity which falls outside the scope of Union law;
    b. by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU ("Specific provisions on the common foreign and security policy");
    c. by a natural person in the course of a purely personal or household activity;

71 Considerandum n. 26 GDPR

72 This was already part of the old framework, i.e. Directive 95/46 (see its Considerandum 43). The CJEU interpreted it, outlining that "for information to be treated as 'personal data'[…], it is not required that all the information enabling the identification of the data subject must be in the hands of one person" (judgement of the 19 October 2016, Breyer, C-582/14, EU:C:2016:779, para. 43).

73 Considerandum n. 26 GDPR. In any case, according to the CJEU, means are never reasonably likely to be used to identify the natural person "*if the identification of the data subject* [is] *prohibited by law or practically impossible on account of the fact that it requires a disproportionate effort in terms of time, cost and man-power, so that the risk of identification appears in reality to be insignificant*" (judgement of the 19 October 2016, Breyer, C-582/14, EU:C:2016:779, para. 46).

74 Article 29 Data Protection Working Party, Opinion 5/2014 on Anonymisation Techniques. Some scholars argue that genuine anonymisation is actually impossible to reach nowadays. See inter alia Berinato (2015).

75 Recital 26, GDPR

76 González Fuster G., Scherrer A. (2015), p. 35

77 Art. 1(3) GDPR

78 GDPR, Article 4, para. 1 (1)

79 GDPR, Article 4, para. 1 (2)

d. by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

- Secondly, the GDPR contains provisions leaving a margin of manoeuvre to Member States for regulating specific kinds of personal data processing. Most notably, Member States can maintain or introduce further conditions in respect to the GDPR, including limitations, with regard to the processing of genetic data, biometric data or data concerning health[80].
- Also, Member States may, by law or by collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context[81]. They may do so, in particular, for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, protection of employer's or customer's property and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship. The GDPR specifies that "*those rules shall include suitable and specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights, with particular regard to the transparency of processing, the transfer of personal data within a group of undertakings, or a group of enterprises engaged in a joint economic activity and monitoring systems at the work place*"[82].

In those cases, the restriction for Member States not to introduce data localisation requirements for reasons related to data protection does not apply. At the same time, the general principles of EU law will apply.

1.2.5 Subjects involved in processing

Processing necessarily requires the involvement of the following subjects: a *data subject*, i.e. the natural person personal data relate to[83], and a *data controller*, i.e. the subject (whether a natural or legal person or any other body) that selects the purpose and means of processing[84] and is therefore accountable for compliance with the GDPR.[85]

The Regulation mentions an additional subject, which may be involved but is not necessary in the context of a data processing operation: this is the *data processor*, i.e. the subject processing the data on behalf of the controller.[86,87] Processing by a processor shall be governed by a contract or other legal act, binding on the processor with regard to the controller, that sets out (i) the subject-matter

80 GDPR, Article 9, para. 4
81 GDPR, Article 88, para. 1
82 GDPR, Article 88, para. 2
83 Article 4(1) GDPR
84 Article 4(7) GDPR
85 Article 5(2) GDPR
86 Article 4(8) GDPR
87 As to the difference between the roles of controller and processor, see Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of "controller" and "processor".

and duration of the processing, (ii) the nature and purpose of the processing, (iii) the type of personal data and categories of data subjects and (iv) the obligations and rights of the controller[88].

Since the processor does not take the fundamental decisions as to the processing operation, it is not, in principle, liable for the damages of the processing, with two notable exceptions. First, the processor is liable where it has not complied with the obligations of the GDPR specifically directed to processors. Those obligations include, *inter alia*, ensuring that persons authorised to process the personal data have committed themselves to confidentiality[89] or deleting/returning to the controller copies of the personal data after the end of the provision of services related to the processing[90]. Secondly, the processor is liable where it has acted outside or contrary to lawful instructions of the controller[91]. In any case, if a processor infringes the GDPR by determining the purposes and means of processing, the processor shall be considered a controller in respect of that processing and shall, as a consequence, be subject to the controllers' liability regime[92].

1.2.6 The data subject's control on personal data: the legal toolkit

The data subject, as the holder of a fundamental right to data protection, is entrusted by the GDPR with a number of rights. Notably, he has the right to obtain information from the controller as to whether data about him are being processed and to receive a copy of those data[93]; to obtain rectification of inaccurate personal data regarding himself[94]; to be forgotten, i.e. to have his personal data promptly erased upon request[95]; to receive the personal data he provided to the controller back in a "structured, commonly used and machine-readable format"[96] as well as to transfer them to another controller without having the former controller obstructing the move.[97]

By the same token, the principles applicable to processing as listed within Article 5 GDPR aim at ensuring the data subject's control over his own data when this undergoes processing. Notably, for processing to be lawful, it must be based on one of the legal grounds exclusively listed by Article 6 GDPR.

Under Article 6 GDPR, processing is only lawful when: (1) the data subject gave his consent to it; (2) it is functional for the data subject to perform a contract or to enter into a contractual relationship; (3) the controller needs it to fulfil a legal obligation; (4) the protection of a vital interest of the data subject or a legal person requires it; (5) the controller needs to carry out a task in the public interest or in the exercise of official authority; (6) the pursuit of a legitimate interest by the controller or by a third party entails it, provided that such controller or third party is not a public authority.[98] Also, pro-

88 Article 28(3) GDPR
89 Article 28(3)(b) GDPR
90 Article 28(3)(g) GDPR
91 Article 82(2) GDPR
92 Article 28(10) GDPR
93 Article 15 GDPR
94 Article 16 GDPR
95 Article 17 GDPR
96 Article 20(1) GDPR
97 Article 20(1) GDPR
98 In this respect, it should be noted that the reference to a legitimate interest as a viable legal basis is of great importance for the development of data markets as it "*allows for a balance between commercial and societal benefits and the rights and interests of individuals*" [Information Commissioner's Office, 'Big Data, Artificial Intelligence, Machine Learning and Data Protection' (ICO 2017) 34].

cessing must be fair and transparent.[99] Furthermore, the collection and processing of personal data is allowed only for "specified, explicit and legitimate purposes".[100]

1.2.7 Supervision

The detailed regulatory system outlined above is enforced by national Data Protection Authorities ("DPAs"). Their tasks, which are not exhaustively listed by the GDPR[101], entail reviewing complaints about violations of data protection law[102], fulfilling an advisory role *vis à vis* national institutions concerning the protection of natural persons' freedoms and rights[103] and investigating on the application of the Regulation.[104]

The GDPR roughly harmonises the authorities' investigative, corrective, authorisation and advisory powers[105] and mandates Member States to add up to the DPA's toolkit the power to signal infringements of the Regulation to national judicial authorities.[106] Moreover, a whole chapter of the Regulation is devoted to ensuring their cooperation and the consistency of their action.[107]

Cooperation in cases of cross-border processing[108] is achieved through (i) the identification of a lead authority as the competent body for monitoring compliance with the GDPR and (ii) the establishment of a set of rules devoted to the regulation of the relationship between the one lead authority and the other authorities involved.

Cooperation is sought, *inter alia*, in the process of elaborating individual decisions. In this case, while non-lead authorities of the Member States affected by the processing operation are obliged to support the activity of the lead authority, this is bound to seek consensus among all affected authorities. For controllers having establishments in multiple Member States, the competent DPA is the one of its State of "main establishment"[109], i.e. "the place where its main processing decisions are taken".[110]

---

99 Article 5(1)(a) GDPR

100 Article 5(1)(b) GDPR

101 Article 57(1)(v) GDPR

102 Article 57(1)(f) GDPR

103 Article 57(1)(c) GDPR

104 Article 57(1)(h) GDPR

105 Article 58 GDPR

106 Article 58(5) GDPR

107 Chapter VII of the GDPR

108 Under Article 4(23) GDPR, cross-border processing is "either the processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or the processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State".

109 Article 56(1) GDPR

110 Gabel D., Hickman T. (2019). More specifically, according to Article 4(16) GDPR, "main establishment" means:
- as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment;
- as regards a processor with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation".
See also Article 29 Data Protection Working Party, Guidelines for identifying a controller or processor's lead supervisory authority, last Revised and Adopted on 5 April 2017, WP 244 rev.01.

The GDPR rules on cooperation also entail the obligation to exchange all relevant information with each other and to provide mutual assistance when needed for purposes of investigation or monitoring of the implementation of a measure.[111] Where appropriate, investigations and enforcement measures can even be jointly implemented by different DPAs, by involving the staff of each of them.[112]

1.3 Public sector data

The public sector produces and holds a wide range of data – covering various areas such as economic, legal or educational topics – which could bring important societal and economic benefits, e.g. through the use of AI to analyse these data and create new and innovative products and services. The value of public sector information (PSI) is constantly increasing: the estimated total economic value of PSI in the EU rose by 57%, increasing from 140 billion Euro in 2010 to 220 billion Euro in 2017.[113] This is mainly due to the increase in the indirect economic value of PSI – i.e. the value of goods and services making use of goods or services based on PSI –, while the direct economic value – i.e. the value of the PSI-based products and services sold – was estimated to have played a smaller role in this increase.

Public sector information vs. Open data

Open data is a subset of Big Data, it designates data which is by definition free to be accessed, used, modified and shared by anyone. Open data can be private or public data. Public sector information refers to a different set of information – i.e. only data collected from the public sector – and contrary to open data, their re-use can be restricted under certain circumstances.

The part of public sector information that is open is commonly referred to as Open Government Data.

A continued increase of the value of public sector information is expected. In 2018, the total economic value of PSI in the 28 EU Member States was estimated to be 236 billion Euro (+7% in only one year), and it is expected to increase up to 672 billion Euro in 2030.[114]

The EU legal framework specifically addresses "public sector information" through its Directive on open data and the re-use of public sector information ("PSI Directive").[115] Adopted in 2019, the PSI Directive replaces the Directive on public sector information[116] from 2003, reviewed in 2013. The new directive must be transposed by Member States by 17 July 2021 and leads to minimum harmonisation in the EU regarding access and re-use of data from the public sector.

The PSI Directive defines "public sector information" as documents held by public sector bodies and public undertakings as well as documents resulting from publicly funded scientific research ("research data").[117] Public sector bodies are national, regional or local authorities, bodies regulated by public law – having a general interest purpose – and associations formed by such bodies or authorities. Public undertakings cover companies active in the sectors of water, energy, postal services, or

111 Article 61 GDPR
112 Article 62 GDPR
113 Deloitte et al. (2018), p. 226
114 Deloitte et al. (2018), p. 401
115 Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information.
116 Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information, subsequently amended by Directive 2013/37/EU.
117 Art 1 (1), Open Data Directive

public, maritime or air transport, where public sector bodies have a dominant influence, e.g. often rail transport or electricity companies.[118]

Under the PSI Directive, Member States should facilitate the availability for re-use – for private or commercial purposes – of public sector data when these data are already accessible under Member States access regimes. Public documents not covered by the Directive include:

- those which are supplied and produced outside the context of a public task or a general interest service – these concepts being defined by national law;
- those related to public activities directly exposed to competition in the water, energy, transport and postal services sectors;
- those subject to intellectual property or personal data protection;
- documents access to which is excluded or restricted under national law – e.g. sensitive data regarding public security issues;
- those held by public service broadcasters, cultural and educational establishments.[119]

On the opposite, the sui generis right for databases which can be awarded to a database owner[120] shall not prevent the re-use of public documents.[121] Thus, even if the data is protected by the sui generis right for databases, public sector bodies holding this right may not exercise it to limit the re-use of the documents of the database. This differs especially from intellectual property rights which prevail over the principles for re-use of public data set out in this Directive.

The PSI Directive does not impose a general obligation to make available data for re-use, public entities are only encouraged to do so.[122] The access regimes to these documents set out by Member States are not impacted by the Directive. However, it does set up some general conditions.

First, documents held by public entities which are accessible must be made available "in any-pre-existing format or language".[123] "Where possible and appropriate", public sector documents shall be available electronically and in "open, machine-readable, accessible, findable and re-usable" formats, which comply "where possible" with formal standards.[124] In this regard, Member States shall encourage the creation of data following the "open by design and by default" principle. Public sector bodies do not have to create or adapt documents if this constitutes a disproportionate effort, nor must they continue the production or storage of certain documents for re-use purposes.

Second, the re-use of public sector data shall generally be free of charge. At most, charges must be limited to marginal costs incurred for the reproduction, provision and dissemination of documents, for the anonymisation of personal data or for the protection of commercially confidential information, and they must be transparent. This limitation of charges to marginal costs does not apply to the public bodies that have to "generate revenues to cover a substantial part of their costs relating to the performance of their public tasks"[125], to libraries, museums and archives, and to public undertak-

118 Art. 2 (1), (2) and (3), Open Data Directive
119 Art. 1 (2), Open Data Directive.
120 Article 7 (1) of Directive 96/9/EC of 11 March 1996 on the legal protection of databases.
121 Art. 1 (6), Open Data Directive.
122 Recitals 23 and 26, Open Data Directive.
123 Art. 5 (1), Open Data Directive.
124 Art. 5 (1), Open Data Directive.
125 Art. 6 (2), Open Data Directive.

ings. For these exceptions, the Directive sets out principles regarding charges for re-use and their calculation: calculations must follow "objective, transparent and verifiable criteria" – as defined by Member States. Also, in this case, the total amount of charges may not exceed "the cost of collection, production, reproduction, dissemination and data storage, together with a reasonable return on investment".[126]

Third, any conditions for the re-use of public sector documents, if at all, must be objective, proportionate, non-discriminatory and justified by a public interest objective. They should not unnecessarily restrict opportunities for re-use or competition. In this regard, Member States should encourage the use of standard licences for the re-use of documents.

The PSI Directive also identifies certain types of data for which specific rules apply. First, Member States shall adopt "open access policies", aiming at an online access free of charge and without restrictions on use and re-use, to ensure the availability of publicly funded research data, while taking into account intellectual property rights, confidentiality and data protection issues.[127] Second, "dynamic data" – i.e. real-time or frequently updated data such as traffic or sensor generated data – must be made available immediately for re-use once they are collected, via Application Programming Interfaces (APIs) or as a bulk download. If making dynamic data immediately available constitutes a disproportionate effort for public sector bodies, the timeframe or the temporary technical restrictions to make these data available must at least "not unduly impair the exploitation of [such data] economic and social potential".[128] Third, the Commission is empowered to list specific "high-value datasets" in a number of thematic categories laid down in the Directive– i.e. geospatial, earth observation and environment, meteorological, statistics, companies and company ownership, mobility.[129] These datasets can e.g. include energy consumption or business registers datasets. As these data can be of high value for the economy and society, they should be available for re-use with minimal restrictions – i.e. free of charge, machine readable, provided via APIs and as a bulk download.[130]

Finally, in order to avoid a "lock-in" and to ensure the non-exclusive access to public sector data, the Directive limits exclusive arrangements which may lead to re-use of public sector information by a small number of private partners only. In principle, the re-use of documents shall be open to all actors, and exclusive rights shall not be granted in agreements between public entities and private parties. However, exclusive rights may be granted when this is considered "necessary for the provision of a service in the public interest"[131] or for the digitisation of cultural resources. In the case of public interest services, such exclusive arrangements must be subject to regular review. In the case of cultural resource digitisation, those arrangements must be limited to ten years.

126 Art. 6 (4) and Art. 7, Open Data Directive.
127 Art. 10 (1), Open Data Directive.
128 Art. 5 (6), Open Data Directive.
129 Art. 14 and Annex I, Open Data Directive.
130 Art. 14 (1), Open Data Directive.
131 Art. 12 (2), Open Data Directive.

1.4 Non-Personal data

1.4.1 Material scope

Non-personal data – defined here as data outside the scope of the General Data Protection Regulation – is subject to the EU Regulation on the free flow of non-personal data (FFD).[132] The Regulation's policy aim is to remove obstacles to the free movement of non-personal data across the EU.

The Regulation applies to providers who supply data processing services to users residing or having an establishment in the EU (e.g. cloud providers) insofar as they process non-personal data. It is irrelevant whether the provider is established in the EU.[133] In case of mixed data sets – i.e. data sets which entail both non-personal and personal data –, the different data-types will be subject to either the GDPR (for the personal data part) or the free flow of data-regulation (for the non-personal data part). When a strict separation of the data is not possible, the GDPR will apply.[134]

1.4.2 Data localisation requirements

As a general principle, Member States must remove all data localisation requirements by 30 May 2021. Such data localisation requirements can be obligations, prohibitions, limits or the like provided for in national laws, regulations and administrative provisions or resulting from national administrative practices which

- impose data processing within a Member State or
- hinder data processing in any other Member State.[135]

As an exception, data localisation requirements can be justified on grounds of public security, but only when they are proportionate in nature.[136] Member States must make any such localisation requirement of a general nature available at a national online single information point.[137] Existing localisation requirements, which Member States wish to keep in place, must be notified to the Commission with grounds demonstrating the justification for reasons of public security.[138]

At the same time, the Regulation ensures that non-personal data – wherever it may be localised in the EU – is available for competent authorities. Access to data by competent national authorities may not be refused on the grounds of that data being processed in another Member State.[139]

1.4.3 Portability

Apart from statutory rules on data localisation requirements by public authorities, the free flow of data Regulation does not entail similar rules regarding private factors which may hinder the free flow of data. Professional users should be able to switch cloud service providers in an easy way, preventing a lock-in effect. However, the Regulation does not entail any direct requirement in this regard but

132 Regulation (EU) 2018/1807 of 14 November 2018 on a framework for the free flow of non-personal data in the European Union.
133 Article 2 (1) (a), FFD Regulation
134 Article 2 (2), FFD Regulation
135 Article 3 (5); Art. 4 (1) FFD Regulation
136 Article 4 (1), FFD Regulation
137 Article 4 (4), FFD Regulation
138 Article 4 (3) , Regulation
139 Article 5 (1), Regulation

calls upon the Commission to encourage and facilitate the development of "self-regulatory" codes of conduct by cloud service provides.[140] These codes should cover:

- best practices for facilitating the switching of service provider and the porting of data;
- minimum information requirements to ensure that professional users have sufficient information to assess a service pre-contractually regarding such switching; and
- approaches to certification schemes that facilitate the comparison of data processing products and services for professional users.

The Commission shall encourage service providers to complete the development of the codes of conduct by 29 November 2019 and to effectively implement them by 29 May 2020.[141] The Commission is required to evaluate their impact by 29 November 2022.

1.5 Reality: Mixed datasets

A mixed dataset is a dataset consisting of both personal and non-personal data. It raises, as such, questions as to whether it falls under the scope of the GDPR or of the FFD Regulation. This is particularly relevant as most datasets used in the data economy are mixed.[142]

The problem is addressed by Article 2 (2) FFD Regulation. Under this provision, in the case of a dataset composed of both personal and non-personal data (i.e. mixed), the FFD Regulation exclusively applies to the non-personal data part of the dataset. However, where personal and non-personal data in a dataset are "inextricably linked", the FFD Regulation "shall not prejudice" the application of the GDPR[143].

The data can be defined as inextricably interlinked when the dataset "contains personal data as well as non-personal data and separating the two would either be impossible or considered by the controller to be economically inefficient or not technically feasible. For example, when buying CRM and sales reporting systems, the company would have to duplicate its cost on software by purchasing separate software for CRM (personal data) and sales reporting systems (aggregated/non-personal data) based on the CRM data".[144]

For mixed and intrinsically linked datasets, this will generally mean that data localisation requirements by Member States are subject to the rules of the GDPR, i.e. Member States may impose them, as long as they do not do so for reasons of data protection and as long as they are compatible with the provisions on the fundamental freedoms and the permitted grounds to derogate from those freedoms.[145]

---

140 Article 6 (1), Regulation

141 Since the adoption of the FFD Regulation, the Commission has encouraged the establishment of two cloud stakeholder working groups: the working group on cloud switching/ porting data (SWIPO) – with subgroups for Infrastructure-as-a-Service (IaaS) and for Software-as-a-Service (SaaS) cloud services – and the working group on cloud security certification.

142 EU-Commission (2019), p. 8

143 See also Considerandum n. 8 FFD Regulation, according to which „[t]he legal framework on the protection of natural persons with regard to the processing of personal data, and on respect for private life and the protection of personal data in electronic communications and in particular Regulation (EU) 2016/679 of the European Parliament and of the Council […] [is] not affected by this Regulation".

144 EU-Commission (2019), p. 10

145 EU-Commission (2019), p. 13

2 Secondary data markets: The economic case

2.1 Economic advantages of data sharing and (re-)use

The exchange of data between businesses features a number of advantages.[146,147]

First, data exchange has the potential for productivity gains for both data providers and data users. Several actors within one value chain may share data to allow for a better coordination of production processes. This may increase efficiency and lower the total costs of production.

Second, data sharing may boost innovation. Data holders may not fully realise the full potential of the data they hold. Third parties, however, may be aware of the potential and have the technical means to generate added value upon re-using the data holder's data, e.g. in combining it with data generated by others.

Third, the rapid uptake of artificial intelligence, machine learning and data analytics technologies increases the value of big datasets tremendously. Keeping data in silos and not opening them up for third party usage limits their economic potential. Pooling data from various sources allows those technologies to produce new insights that may form the basis for new products and services.

Fourth, the possession of large datasets by one economic actor might serve as a market entry barrier for other companies. If such data is 'essential' for market entry, the lack of access to it may result in the absence of effective competition in the products or services market of the data holder. Regulated data sharing may thus be a means to enhance competition (more one competition questions see Chapter III below).

Fifth, data sharing has also a societal dimension. New technologies not only offer potential for better products and services, but also may help to gain knowledge about how to tackle certain societal challenges like curing diseases, fighting climate change or solving famines.

2.2 The characteristics of data

2.2.1 Data is non-rival in consumption

Standard economics usually differentiate between four types of goods – private, public, common and club goods. This classification depends on two distinctive factors (see Table 3):

- rivalry, i.e. the consumption of the good by one user reduces the ability of another user to consume it;
- excludability, i.e. anyone who is unwilling to pay can be excluded from consuming the good.

Data is non-rival in consumption: The fact that data is being used by a consumer does not hinder another consumer from using it as well.[148] Data supplied by a business may be used by many other businesses for many different purposes at the same time and without any "loss of information content".[149]

146 Netherlands Ministry of Economic Affairs and Climate Policy (2019)
147 The presented list is by no means complete, but only a selection.
148 Duch-Brown, N., Bertin M. and Mueller-Langer F. (2017), p. 12
149 Id.

Theoretical classification of goods	Excludability	Non-Excludability
Rivalry	Private Goods (Cars, Books, Drinks…)	Common Goods (Forests, Fisheries…)
Non-Rivalry	Club Goods (Cable TV, Gym Membership…)	Public Goods (Defence, Fire brigade)
	Data	

Table 3: Theoretical classification of goods

The fact that data is non rival in consumption implies that it is often welfare-enhancing to share it with other consumers/businesses. This is all the more true since data producers may not have full knowledge about the value of its data and its potential use cases. Moreover, sharing data allows others to merge the provided data with data from other data suppliers, enabling them to offer new products and services with a welfare enhancing effect.[150]

Whether data is excludable in consumption is more difficult to answer. Although data ownership rights are often not conclusively regulated, there tends to be a de-facto excludability of the use of data. Physical, technical and security measures often enable data producers to exclude others from accessing and utilising "its" data.[151,152] Even though this can be associated with considerable costs, is not always legally enforceable and hence does not protect data to the same degree as a formal ownership right would, it establishes "factual ownership".[153] Without explicit consent of the factual data possessor, third parties are often not able to access data controlled by its producer.

According to the usual classification of goods (see Table 3), data subject to this de-facto excludability in combination with non-rivalry in consumption would qualify as a "club good".

In economic theory, club goods like a gym membership build on the assumption that an increase in members of the club lowers the average costs of the provision of the good and thus also the price of consumption for each member. However, adding members to the club leads to crowding and at some time even to congestion. Thus, the marginal benefit of an additional club member declines with the number of members (at least above a certain level).[154] To avoid congestion, clubs may hence limit the number of admissible members.

Data can be seen as club good in that an increasing number of (non rival) data users (similar to the members of the gym) lowers the average cost of producing the data and hence the price for the individual users. There may, however, be a limited amount of use cases for the purchased data.[155] An additional buyer may not cause congestion like in a gym but may lower the marginal benefit of possessing the data for former buyers in case new buyers use the data for similar purposes. Thus, com-

150 Schweitzer, H. and Peitz, M. (2017)
151 Kerber (2016)
152 Drexl et al. (2016)
153 Willems (2017)
154 McNutt (1999)
155 The amount of potential use cases may not only depend on the purchased data from one data producer. If a buyer is able to purchase several datasets from one or several data seller, the merging and analyses of the combined data likely increases the amount of potential use cases. In this case, the marginal benefit of possessing data does not diminish very soon.

parable to a club, it might make sense for de-facto data owners to limit access to its data to keep it valuable.[156]

However, not all data can be seen as club good. Some data (e.g. public data) may be not excludable, meaning the producer of the data may have no means to exclude others to use its data. The dramatic reduction in the cost of conversion, copying and transmission of digital content between carriers significantly reduces the ability to exclude others from using data.[157] Data which is both non-excludable and non-rivalry in consumption qualifies as a public good.[158]

A major problem of public goods is that free riding is likely to occur: As users cannot be excluded from consumption, they have an incentive not to pay for the costs of data production. Assuming a positive cost of data production, the level of data production will then be suboptimally low from a social perspective.[159] The extent of this problem depends upon two factors:

- Value attached to the data by the data producer: A producer of data may attach value to the data he produces and may hence be willing to carry the production cost of data, even though he cannot exclude others from using his data. The higher the data producer's valuation, the closer data production will be to the social optimal level.
- The cost of data production: Data are often generated as a by-product of other processes and may not be the main business focus.[160] Depending on the case, the marginal cost of data production may be very small. Once a data producer has incurred the fixed costs of data production – e.g. because he values data for his own use or because fixed costs were incurred for another process and data production is just a by-product – , the fact that he cannot exclude others to use the same data may not have a significant impact on the additional production of data. The lower the marginal costs the more likely it is to reach a data production close to a social optimal level.

156 Limitation may include the means of price differentiation.
157 Duch-Brown, N., Martens B. and Mueller-Langer F. (2017), p. 12
158 OECD (2015)
159 Pindyck S. and Rubinfeld L. (2005)
160 Goodridge, P. R., Chebli O. and Haskel J. (2015)

2.2.2 Economies of scale

Economies of scale arise when the marginal costs of producing decline as production increases (see Figure 17).

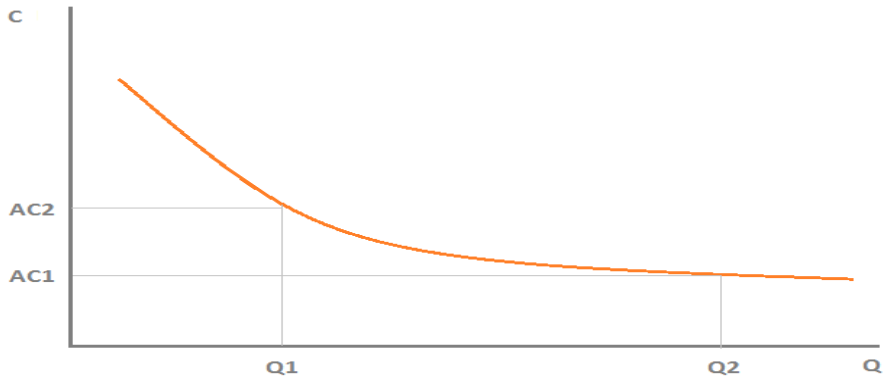

Figure 17: Economies of scale
Source: cep

Digital markets are often characterised by economies of scale. This is so because of

- high fixed and low marginal costs: The cost of producing the first copy of an information good may be substantial, but the cost of producing (or reproducing) additional copies is negligible.[161,162]
- the special role of data in some digital value chains, especially with big data, machine learning or artificial intelligence: The quality of these digital services becomes more reliable as the size of the underlying dataset increases and the variation in the data decreases.[163] Nevertheless, the size of this effect tends to decline the bigger the dataset grows.[164,165]

2.2.3 Perishability of data

Data is often perishable, i.e. it loses value over time.[166] While some data has a lasting value – e.g. data on individuals' names and birth dates, which do not change often or at all – other data is short-lived.[167] The perishability of data regularly depends on its exact use: data on car driving may have a high instantaneous value during rush hour as navigation software may advise drivers to take another route to bypass a traffic jam. Once rush hour has passed, the value of this data for navigation will be limited. On the other hand, the traffic data may still have value for the provider of the navigation software that collected the data, as he might be able to predict future traffic jams more easily and

161 Shapiro C. and Varian H. (1998), p. 3
162 Setting up a search engine that collects data from search queries is costly (high fixed costs). Only such expensive initial investment allows the provider to be able to gather his first data and the information related to it. The collection and analysis of queries by more user is, then, in fact, costless (low marginal costs) and each query creates benefits for the provider as he may use machine learning.
163 Martens, B. (2018), p. 9
164 Martens, B. (2018)
165 The eleventh person using a company's search engine is likely to train the algorithms to a greater extent in gaining new insights than the 500.000th user.
166 AGCOM (2018), p. 35
167 Burri, M. (2019), p. 13

learn from past patterns concerning driving behaviours. However, he has to gather such data over a longer time horizon to derive such benefits: The sum of the values of a single datum taken at a given moment is very different (and much lower) than the value of data taken as a whole and in a wider time interval.[168,169]

2.3 Conclusion

Data sharing and re-use is set to generate considerable economic and societal gains. It is hence important to allow the establishment of secondary markets for such data. At the same time, three distinct characteristics of data and the digital economy offer economic reasons for abundant pooling and sharing of data. First, data is non-rival in consumption. Its offering enables the use of data by a high number of users, even simultaneously and for very different reasons. Non-rivalry serves as a multiplicator and underlines the benefits of a deep and functional supply of data. Second, data supply is often governed by economies of scale. This as well gives reason to support a well-functioning and abundant supply of data. This goes all the more as ample data is needed to increase the quality of big data-related products. Third, to a certain degree, data is perishable and digital technologies may need a steady inflow of fresh data, which presupposes a rich supply of data.

3 Secondary data markets: The obstacles

In the following, we identify some of the most important obstacles to the development of secondary data markets regarding personal, public and non-personal data.

3.1 Personal Data

The GDPR has updated and granted more power to EU data subjects in relations to their personal data, laying out detailed data protection rights and additional transparency requirements. Further emphasis needs to be put on the GDPR's effective implementation, particularly in the context of AI, IoT and the data sharing economy. It is therefore crucial to identify in which terms the establishment of a market for business data can be combined with an effective enforcement of the GDPR.

3.2 Public Data

Although the PSI Directive in its 2019 review has addressed a number of obstacles to the availability of data from public sector entities, obstacles remain.

First, the lack of standardisation of data and interface formats is identified as a remaining barrier for the availability of public data.[170] While standardised interoperable data formats are crucial to facilitate access and re-use of data, the PSI Directive provides for few requirements only regarding open standards in the conditions for re-use by stating that "both the format and the metadata shall, where possible, comply with formal open standards".[171] Some sector-specific regulations already exist, e.g. the INSPIRE Directive[172] which establishes a common infrastructure for spatial information in the EU.

168 AGCOM (2018).
169 Graef, I. (2015), p. 483.
170 Bundesministerium für Wirtschaft und Energie (2019a)
171 Art 5(1), PSI Directive
172 Directive 2007/2/EC of the European Parliament and of the Council of 14 March 2007 establishing an Infrastructure for Spatial Information in the European Community (INSPIRE)

Second, the PSI Directive covers a number of public bodies and undertakings, but private companies are not covered by these requirements regarding re-use of data. This may pose an obstacle to public data sharing in those cases where public authorities entrust the provision of services of general economic interest (SGEI) to private sector companies.

3.3 Non-Personal Data

3.3.1 The state of secondary business data markets in the EU

Empirical data on the extent to which European companies share, sell or buy data is rare and not conclusive. According to a Deloitte study, 78% of European companies claim to share data with third parties, be it for free or at a cost.[173] At the same time, a non-representative subset of 100 business models points to data sharing in only 22% of the cases.[174] The authors conclude that limited data sharing is an issue for the most innovative companies and in selected sectors only, but that the problem can be expected to grow in the future.[175] Companies with a large data pool use data in-house and do not regularly offer that data on the market. Hence, the exchange of data between companies remains very much the exception, not the rule.[176]

In an international comparison, the EU seems to be lagging behind concerning the state of its secondary data markets as well. In lack of data on B2B data sharing, proxy indicators – such as the value of data markets, the incidence of the data economy on GDP and the number of data suppliers in the EU, the US, Japan and Brazil – show that the EU is not a frontrunner. The value of the data markets (162,2 billion €) and the share of the data economy on GDP (1,17%) in the US are more than double the EUs' size (71,6 billion € and 0,52%) in 2018. Furthermore, keeping in mind that the gross domestic product of the whole EU is roughly four times the size of the one of Japan[177], the value of the data markets in Japan (29,3 billion €) is much higher than the EUs' data markets (71,6 billion €) in relative terms (see Table 4).[178]

Data markets indicators 2018	EU	USA	Japan	Brazil
Value of the data markets (in bill. €)	71,6	162,2	29,3	7,6
Share of data economy (in % GDP)	0,52	1,17	1,05	0,22
Number of data suppliers	272.200	309.000	105.100	37.300

Table 4: Data market indicators
Source: International Data Corporation (IDC) and the Lisbon Council (2019)

The backlog is also reflected insofar as only 6,3% of companies in the EU are taking part in B2B data sharing and (re-)use. Furthermore, the interest of companies to open up their data for third parties is limited. Only 18% (40%, 33%) of small (medium-sized, large) undertakings are interested or active in sharing their data with others. The interest in accessing data from third parties is rather weak as well. It ranges from 23% for small companies to 12% for medium-sized and 9% for

173 Deloitte (2017), p. 62
174 Id. p. 63
175 Id. pp. 63-64
176 Communication by the EU-Commission, Building a European Data Economy, COM (2017) 9, p. 9
177 International Monetary Fund (2019)
178 International Data Corporation (IDC) and the Lisbon Council (2019)

large companies. On the other hand, the mutual exchange of data – share and access – is much more popular. 59% of the small, 48% of the medium sized and 57% of the large firms are interested or active in such an approach.[179]

In the following, we offer a series of general explanations explaining why supply and/or demand of non-personal data may be limited.

3.3.2 Strategic risks

Companies may abstain from supplying data to third parties as they may fear losing or compromising their competitive advantage when this data becomes available to their competitors.[180] It may not always be easy for potential data suppliers to assess the economic potential to competitors of the data they are considering to supply. This goes all the more as the combination of data supplied by a company with data supplied by others – the supply of which the initial supplier may not be aware of – may enable competing companies to strengthen their competitiveness vis-à-vis the original supplier of data.

Besides problems in identifying the potential of data for a competitor, it may also be difficult for a company that considers offering its data to others to identify the competitors themselves. Technological changes may cause the entrance of new players in the market and data which is of little value to traditional competitors may be of high value to those new entrants. Thus, the number of potential competitors may be very high, and they may be difficult to identify.

Thirdly, companies considering the supply of data may want to prevent that the supply of data leads to the establishment of new markets. This may be most relevant for aftermarkets. Especially manufacturers of industrial goods may want to prevent that the data supplied opens up the market for follow-up services such as maintenance, repair and spare parts.[181] In a similar way, companies may decide not to supply data as they may expect to profit in the future from exclusive access to that data regarding applications in markets which do not yet exist.[182]

Empirical research points out that strategic doubts are the main barrier for companies to supplying data. For more than half (52%) of the companies, strategic concerns constitute a considerable, very important or even blocking barrier to sharing data. These companies are afraid of sharing sensitive information and losing their competitive advantage without even realising it.[183] 15% of the surveyed companies even rules out supplying data because of these concerns.

3.3.3 Technical problems

Data supplied – and demanded – by companies may be very diverse and it is unlikely to be a homogeneous good. This goes both for the very subject of the data and for the technical data format it takes. Hence supply and demand may have difficulties in meeting each other, as both sides often have to invest money in making an exchange technically possible.

179 Deloitte (2017)
180 Id. p. 10
181 Schweitzer, H, and Peitz, M. (2017), p. 56
182 Cf. Netherlands Ministry of Economic Affairs and Climate Policy (2019), p. 13 and 14
183 Deloitte (2017), p. 78-79

There are various dimensions to this problem. One issue is the process of data curation. It does not only absorb human engagement, but is often technically challenging, as there may well be limits to data stocking and the ability to process and keep large volumes of data up-to-date.[184] A second obstacle is the issue of a lack of interoperability between datasets and information systems that factually inhibits the valuable exchange of data. Also, incompatible standards are an issue or different systems of data storage. The applied technical solutions might act also as barriers. A lack of trust in such technical solutions, e.g. with respect to cybersecurity risks may inhibit data trading.[185]

Empirical research shows a diverse picture with regard to technical barriers. According to the Deloitte study, 6% of the firms claim that technical issues are a blocking factor for them to share data. At least 23% state that these issues are an important factor.[186] Another study found technical barriers and associated costs to be the main barrier for B2B data trading with 73% of responding companies (note: only 129 firms participated in the survey) pointing to that issue.[187] The same study also revealed that the lack of standardisation and interoperability constitutes a barrier to data sharing, mostly in the energy and the agricultural sector. The automotive, telecoms and mobile health sector are affected to a lesser extent.[188] In a representative survey among German companies, 72% of firms that are generally willing to share data mention the lack of common standards as a serious or rather serious barrier to data sharing.[189,190]

3.3.4 Uncertainty

Data trading is also hindered by a lack of certainty. This problem has various dimensions:

First, data holders may not be aware of the legal status of 'their' data as there is no ownership right or other property type right for data. Thus, market actors may be uncertain about what can and what cannot be done with data and this may inhibit its exchange. Whether or not the uncertainty about the ownership of data is a major impediment to sharing data is being discussed widely. Among respondents to a targeted consultation by the Commission, 80% of the businesses signalled that the question on who actually 'owns' data is important or very important to them.[191] On the other hand, another study stipulates that data ownership is a blocking factor or a very important or considerable barrier for only 45% of the respondents. More than half (55%) deem it to be not that important.[192] Among companies not yet active in B2B data sharing business, another study found 62% of the respondents being concerned about the legal uncertainty around data ownership, while this concern diminished to 54% among those respondents that claim to share data already.[193] Unclear ownership rights are prominent in Germany, where more than 83% of companies that are ready to trade with data see this aspect as a (major) impediment.[194] On a more general basis, other legal unclarities may

184 Everis (2018), p. 75
185 Id. p. 26-27 and 75-76
186 Deloitte (2017), p. 79
187 Everis (2018), p. 75
188 Id. p. 26
189 1.104 companies participated in the study. 467 of them are in general willing to share data.
190 IWConsult (2019)
191 European Commission (2015): DSM Free Flow of Data Initiative and emerging issues of data ownership, access and usability, p. 8., see: http://ec.europa.eu/newsroom/document.cfm?action=display&doc_id=12205
192 Deloitte (2017), p. 76
193 Everis (2018), p. 45 and 74
194 IWConsult (2019)

hinder data sharing as well. Intellectual property rights, data protection issues, trade secrets law and contractual rules may further complicate data exchange.[195]

A second issue that creates uncertainty is the aspect of data misuse and leakage. Potential data seller may not be willing to share data, because they may not be able to control the use of the data by data purchasers. They may fear that buyers do not keep the data within their sphere of influence but may leak or resell them to other parties. As a result, data may get in the wrong hands from the perspective of the potential data seller. What is more, the original data seller may have difficulties monitoring the use of the data sold as traceability or monitoring of data usage is both costly and technically challenging. The breach of data licencing agreements is hence not very well observable by data sellers. Consequently, potential data sellers may abstain from data sharing to avoid such unintended data misuse.[196] Research shows that 46% of the firms participating in a survey – not yet engaging in B2B data sharing – stated that the ability to track the usage of data would increase their willingness to share data.[197]

The question of data misuse or leakage has also to do with uncertainties about the suitability of licencing conditions/contract terms that usually govern the rights and obligations for the exchange of data between data sellers and buyers. Doubts regarding the enforceability of data sharing contracts are widespread and clear terms and conditions may be helpful in establishing the trustful relationships necessary for promoting data exchange. 42% of not yet engaged B2B data traders would favour more contractual certainty. This would increase their readiness to share data. Interestingly, however, licencing conditions are no blocking factor for them to enter the B2B data trading business.[198]

Third, liability is a subject matter, as well. Each party to a data sharing contract seeks to minimise liability risks. Data sellers typically have in interest in the data not being misused or leaked by the buyers and the data being secured appropriately and shielded against e.g. cybersecurity risks. Thus, sellers will demand assurances by the data purchasers which guarantee the fulfilment of such demands. On the other hand, data buyers are mostly interested in the validity of the data they purchase. Incorrect data may increase their liability risk, e.g. if they establish new products or services based on erroneous input.[199] As an example, in the health sector, patients being treated wrongly as a result of research based on false data inputs may cause large liability risks. For 28% of those companies that do not share data (yet), uncertainty about safety, security and liability conditions related to the technical process of sharing data is an issue.[200]

Summarising, uncertainties with regard to ownership rights on data, data misuse or leakage and liability risks are an important barrier to B2B data sharing. It is a blocking factor for 12%, a very important barrier for 25% and a considerable aspect for at least 35%. Only roughly 30% do not have any concerns in this regard.[201]

195 Deloitte (2017), p. 74
196 Kerber, W. (2016)
197 Everis (2018), p. 46
198 Id. p. 44 and 45
199 Deloitte (2017), p. 81-82
200 Id. p. 44
201 Id. p. 79

3.3.5 Valuation problems

In traditional neoclassical economics, the value of an economic good and, thus, its price is usually determined by supply and demand. Whether the good is traded or not depends on the willingness one party to sell the good at a certain price and the willingness of another party to pay the price. The establishment of markets for economic goods[202] like data is, however, often difficult. One of the reasons for this is the difficulty in attaching a value to data.[203,204] This may be the case for a number of reasons[205]:

- Buyers of an information – here: data – may not know the value of an information until they actually know the information (Arrow's information paradox).[206] Unlike many other goods, it may be challenging to reduce buyers' uncertainty by previewing or testing the information before consumption takes place.[207] As a result, buyers without knowledge about the information may not be willing to pay the purchase price. Having offered them this knowledge prior to purchase, they will no longer see the necessity to purchase.[208] Consequently, the markets for information goods, respectively data, are prone to fail as long as data sellers cannot sufficiently and credibly describe the value of data to buyers without disclosing the full data set.[209,210] In other words, the value of data is not determinable ex ante, but only after it has been consumed and put to use.[211] Data with such characteristics can be qualified as an experience good.[212]
- The asymmetric distribution of information between potential data sellers and buyers hinders the valuation of data. Typically, sellers of data possess more information about the data than potential buyers. This may lead to adverse selection problems. In lack of exact information, buyers are willing to pay a price for data of average quality only. As the seller knows the true quality of his information good, he will not be willing to sell data of a quality above average. Potential buyers will anticipate this fall in average quality and will adapt their willingness to pay downwardly. In the end, the market for the information good will collapse and data selling will not take place at all.[213,214]
- Although selling data may include its transfer to third parties, it does not necessarily imply the original seller may no longer dispose of it. This non-rivalry is uncommon for economic goods and may complicate the valuation of data. The value of data may depend on the num-

202 Among economist there has even been a debate on whether information or data can actually be considered an 'economic good' at all. Bates argues that it is an economic good as it "can be transferred, has some utility and is capable of having a value attached to it" [Bates, B. J. (1990), Krippendorf (1985)].
203 Linde, F. (2009)
204 Vomfell, L. et al. (2015)
205 There are much more features of data that aggravate its valuation, i.a. its perishability (see page 30) or the pattern of its cost of production (high fixed costs, low variable costs).
206 Arrow, K.J. (1972)
207 Vomfell, L. et al. (2015), p. 12
208 Dewenter, R., Lüth, H. (2019), p. 43
209 Rusche, C. and Scheufen M. (2018), p. 16
210 Kerber (2016) argues that "although such problems cannot be ruled out in regard to data, in most cases it can be assumed that the data can be defined and described sufficiently for a buyer to assess their value (without revealing them in detail). Therefore the information paradox is presumably not a huge problem for commercialising data". [Kerber, W. (2016), p. 12]
211 Bates, B.J. (1990)
212 Deloitte (2017), p. 93
213 Vomfell, L. et al. (2015)
214 Akerlof, G.A. (1978)

ber of buyers or on whether the seller still works with its data and this information may not be available (ex-ante) to each and every buyer. In this way, a buyer cannot be certain that data keeps its stock value after the acquisition[215], which aggravates the problem of determining a certain value for the data in the first place.[216] Regularly, the stock value is about to decrease with the number of buyer.

- High uncertainties regarding to the potential use cases of their data may make it difficult for data sellers to value their data. In effect, this problem is an inverse market for lemons problem and data sellers will react to it by charging average prices, which will cause potential buyers to cease to demand for all use cases with a value below this average. Sellers will react to this and will again raise prices to a new (and higher) average use case. In this way, supply and demand will fail to meet and the market will fail.[217]

Even though theory shows a variety of challenges associated with attaching data an appropriate price, the issue does not seem to be one of the main obstacles for data sharing. More than 50% of survey respondents state that valuation of data is not or only a minor barrier. Nonetheless, still more than 30% claim it to be a blocking, very important or considerable factor.[218] With regard to companies not taking part in the data sharing business, only 11% mentioned data valuation as a big obstacle.[219]

Excursus: Approaches for a proper valuation of data

One can broadly distinguish three main approaches for evaluating data:[220]

- Market-based procedures: Using this approach, the value of data depends on its selling price on active competitive markets, which means that it is dependent on supply and demand on those markets.
- Cost-based procedures: Using this approach, the value of data is determined by its costs of production, procurement, provision, sharing and quality control.
- Utility-based procedures: Using this approach, the value of data depends on the financial benefits it generates over its total time of usage.

Each of the three procedures for valuing data properly has its own preconditions, advantages and disadvantages:[221]

- In general, market-based procedures are most reliable. However, they can only exploit their full potential given functioning and competitive data markets, which are quite seldom as of today. Without such liquid markets, there is also no market prices that may be a reference point for pricing one's own data. Furthermore, data often miss comparability as they are relatively heterogenous.

215 Id. p. 12
216 Bates, B.J. (1990)
217 Deloitte (2017), p. 93-94
218 Id. p. 78-79
219 Everis (2018), p. 44
220 Krotova, Rusche and Spiekermann (2019), p. 27 and 28
221 Id., p. 46-48

- Cost-based procedure are usually quite simple in the sense that they are strictly backward-looking. This backward orientation has its drawbacks. First, it is often difficult to determine historical costs ex post. Second, the backward perspective conflicts with the fact that data are usually experience goods (see also above). That means that its value is regularly underestimated as the look back to the past does not incorporate its potential future value. And third, the utility of the data is not necessarily reflected in cost calculations.
- Utility-based procedures are the most complex and costly. They are forward-looking, risk-based and holistic in the sense that they take the whole data lifecycle into account. On the other hand, these methods are relatively subjective and dependant on assumption and estimates.

Box 1: Approaches for a proper valuation of data

3.3.6 Market design

The design of data markets may hinder B2B data sharing. In the following, we stick to a classification presented by Koutroumpis et al. focussing on the number of parties on each side of the market and elaborating on the consequences for B2B data trading for each category (see Table 5).[222]

Categorisation of data markets	Design	Exchange terms	Liquidity	Transaction costs	Provenance	Excludability
One-to-one	Bilateral	Negotiated	Low	High	Clear	Medium
One-to-many	Dispersal	Standardised	High	Low	Unclear	Low
Many-to-one	Harvest	Standardised	High	Low	Unclear	Low
Many-to-many	Multilateral	Standardised or negotiated	High	Low	Medium	Low
Most appropriate B2B data sharing set up	Multilateral	Standardised	High	Low	Clear	Medium-High

Table 5: Categorisation of data markets
Source: Koutroumpis et al. (2017), p. 16, 20 and 21 and cep

- **One-to-one**: In this scenario, a data seller and a data buyer meet in a bilateral relationship. The seller may have gathered the data by itself or may re-sell data bought from another party (data brokerage).[223] Usually, bilateral contracts have the shape of licencing agreements, i.e. the seller grants the buyer a right to use its data but retains access to the data. Thus, both parties are able to use the data at the same time.[224] One-to-one relationships cause high transaction costs (e.g. costs for finding a suitable trading partner, negotiation costs) and the difficulty in finding contracting parties leads to low liquidity markets. One-to-one relationships offer two important advantages: First, the source – and hence the quality – of the data can be ensured comparably easy (clear provenance) and second, it is comparably easy to exclude third parties from gaining access to the data, which may be important for secretive da-

222 Koutroumpis, P., Leiponen A., and Thomas L. (2017)
223 Id. p. 17
224 Dewenter, R., Lüth, H. (2018), p. 30

ta.[225] As a result, most of today's B2B data trading is taking place in a one-to-one design, most likely due to the features provenance and excludability. However, the high transaction costs and low thickness of the market limit its size.

- **One-to-many**: In this scenario, one party sells data to many buyers (dispersal marketplaces). Like in a one-to-one relationship, such marketplaces are one-sided markets in the sense that there are no interdependencies between different user groups.[226] Contracts in the one-to-many scenario are usually not negotiated individually but are more standardised, which reduces transaction costs. Data exchange regularly takes place using application programming interfaces (API). Given low transaction costs, dispersal marketplaces tend to be more liquid, if they attract enough buyers. Whether the quality of the data is ensured in this market design is an open question and depends i.a. upon the level of standardisation of the contracts or the strategic behaviour of the data buyers (unclear provenance). First, in standardised contracts it may be more difficult to describe data quality in a way which is sufficient for each and every buyer. And second, in one-to-many relationships, the data usage by one buyer may lower the value of the same data for other buyers. What is more, in a one-to-many scenario, it may be more difficult to differentiate access rights to data amongst buyers due to standardised terms and conditions. This, however, may be important, e.g. when a seller is concerned about offering competitors access to sensitive data.[227] For B2B data-sharing, the unclear provenance and low excludability may be relevant barriers, even given lower costs than in the one-to-one framework.
- **Many-to-one**: In this scenario, many sellers deliver their data to only one buyer (harvest market). Social networks and search engines serve as examples. Harvest markets often exhibit a two-sided market structure in which sellers offer their data (often for free) to a specific buyer which uses the data not only to improve its own product or service vis-à-vis the seller, but also to serve other clients on adjacent markets. The buyer thus acts as a 'data platform' that serves two distinguished groups of costumers. In this market design, the sellers basically agree in an 'implicit barter' – free services paid with data. Given successful services, liquidity in the markets is high and transaction costs low (as there are usually no individual service contracts). Data quality is an open question as sellers may provide correct or biased data in the absence of control mechanism (unclear provenance). Excludability in this scenario is likely to be low, as sellers do usually have no or limited means to control what buyers do with the data, e.g. whether they resell them and to whom.[228,229] While many-to-one markets are common in the B2C context, its relevance in B2B data sharing is limited given unclear provenance and low excludability.
- **Many-to-many**: In this multilateral scenario, many sellers meet many buyers of data. Data marketplaces[230] or data sharing platforms[231] act as match makers in between those two

225 Koutroumpis, P., Leiponen A., and Thomas L. (2017), p. 17 and 21
226 Dewenter, R., Lüth, H. (2018), p. 30
227 Id. p. 17
228 Koutroumpis, P., Leiponen A., and Thomas L. (2017), p. 18
229 Dewenter, R., Lüth, H. (2018), p. 31
230 "Data market places" facilitate the transfer of data from sellers to buyers. Usually buyers pay a price for the data of the seller and the buyers do not necessarily act at the same time as sellers.
231 "Data sharing platforms" also facilitate the transfer of data from sellers to buyers. However, such transfers are usually free of charge and the buyers may also act as sellers and vice-versa.

groups. As in the many-to-one scenario, the market set-up is two-sided. Data marketplaces act as facilitators of data trades and are an instrument to reduce transaction costs between both market sides. The success of such marketplace mainly hinges upon its governance structure, trust systems, institutional set-up and rules for data exchange, as well as the ability to attract enough participants on each market side. If successful, – investments to establish such platforms are likely to be substantial and efforts by the platform providers are needed to keep it stable due to e.g. adverse selection risks on the sellers' side – liquidity will be high and transaction costs be low. Provenance may, however, be only at a medium level, as data sellers may take advantage of the governance challenges and only provide data with low quality. Buyers, on the other side, may exploit those challenges by e.g. misusing the data. Still, excludability might not be a common feature of such platforms due to standardised contracts, which limits their attractiveness for sellers.[232,233]

For B2B data sharing, all market models presented have their special peculiarities and no model is a perfect match (see Table 5 above). This may only be a barrier to B2B data trading.

As of today, businesses mainly try to gather data internally and only use that specific collected data. External sources are being used seldomly. Data sharing occurs, but mainly bilateral, The trading of data using platforms as facilities is of limited importance so far.[234] A recent study points out that only 6% businesses claim that they use open platforms and marketplaces for sharing data and only 13% see it at as possibility for the future. However, the same study also reveals that 47% of German businesses participating in the study see a lack of marketplaces as a barrier for data trading.[235]

3.3.7 Costs of data sharing

Data sharing causes costs.

First, fixed costs for generating data or for establishing the infrastructure or platforms necessary to transfer data to third parties may be considerable. This includes the costs for production and installation of sensors in machinery, costs for curating data to ensure its quality, efforts to ensure the documentation of the provenance of the data, or costs to allow for interoperability with other computer systems (standardised formats). With respect to personal data, this may also include costs to ensure their proper anonymisation to avoid conflicts with the GDPR.[236,237]

Second, depending on the set-up of the data market, transaction costs are relevant.[238] In this context, costs for searching the right contracting partner(s) (who has vs. wants certain data in which format and to which terms and conditions), for choosing the most appropriate market design (where to exchange the data). Furthermore, costs for finding appropriate contractual arrangements (legal costs) will be relevant (e.g. who pays for damage caused by the data shared or aspects of data (re-)usage and reselling).

232 Koutroumpis, P., Leiponen A., and Thomas L. (2017), p. 19
233 Dewenter, R., Lüth, H. (2018), p. 31-32
234 Schweitzer, H. and Peitz M. (2017), p. 24
235 IWConsult (2019)
236 Kerber, W. (2016)
237 As stated above, the costs of sharing data once infrastructure is in place are usually low (low variable costs).
238 This is especially true for one-to-one bilateral relationship (see also section 3.5).

Third, ensuring sufficient data security to cope with cybersecurity risks may cause significant costs.[239]

Fourth, employees may not possess the comprehensive knowledge necessary for useful data sharing, causing considerable training costs.

Fifth, lock-in costs may be relevant. Once a business has selected a bilateral contracting partner(s), marketplace or platform, it may be difficult to switch to other partners, marketplaces or platforms due to contractual barriers or data portability problems. Thus, the prospect of lock-in costs may inhibit data sharing in the first place.

Sixth, the price for data is an obvious and direct cost. High data prices may lead to inhouse production given opportunity costs.[240,241]

Businesses are interpreting the relevance of costs for sharing data very differently. A study revealed that in case of randomly chosen companies that (want to) access and (re-)use data (demand side), the costs of technical implementation, the costs to acquire the right skills and administration are most relevant. For companies that are already intensive data users, however, the costs of buying the data and for receiving legal advice matter the most. If data sharers are considered (supply side), the costs of technical implementation, costs of acquiring the right skills and administration costs are critical factors for the randomly chosen firms, while costs of acquiring the right skills and administration costs are most decisive for intensive data suppliers (see Table 6).[242]

Most relevant cost factors	Cost factor 1	Cost factor 2	Cost factor 3	Cost factor 4
Demand side	**Technical implementation** Very high relevance: 2% High relevance: 37%	**Acquiring of skills** Very high relevance: 3% High relevance: 24%	**Administration** Very high relevance: 4% High relevance: 19%	
Supply side	**Price for data** Very high relevance: 76% High relevance: 14%	**Legal advice** High relevance: 94%	**Acquiring of skills** High relevance: 81%	**Administration** High or very high relevance: 81%

Table 6: Costs associated with sharing data
Source: Deloitte (2017)

The costs of data sharing was, however, not often said to be a blocking factor or even very important barrier (supply side).[243] On the contrary, the costs of data was identified by 80% of intensive data users as a blocking factor and 76% as a very important barrier. Randomly chosen companies only see the costs for data in 48% as an issue and only 11% believe costs to be a very important or blocking factor.[244]

239 Investments to cope with cybersecurity risks may also involve the decision to instruct cloud service providers to deal with those risks, if data is stored with such providers.
240 Everis (2018)
241 Deloitte (2017)
242 Deloitte (2017), p. 64 and 65
243 Id. p. 79
244 Id. p. 80

3.3.8 Lack of skills and workforce

Companies that want to enter the B2B data sharing business must have enough knowledge, capabilities and skills to do so. In this regard, first, expertise is needed in the sense that a company is capable of assessing the possibilities its data brings.[245] Second, technical skills have to be mentioned. Manpower is, e.g. needed to build an appropriate infrastructure and internal processes to be able to exchange data. Furthermore, legal expertise is required to deal e.g. with data protection questions or liability issues. Especially, data buyers may also need data scientists that help to extract as much value out of purchased data as possible.[246] At the very beginning, the job market must also be able to deliver the adequate workforce to fulfil such jobs.

Consequently, a lack of skills and workforce – already perceived as a cost factor in the former section – may inhibit data sharing, especially for small and medium-sized companies that cannot draw from a large pool of employees.

Among companies that claim to already share data, 38% declared that a shortage in skills is relevant for them, a survey in a study revealed.[247] 18% of those that do not yet share its data state that a lack of knowledge is impeding them from engaging in the B2B data sharing business and 29% declare that they were willing to start trading data if "availability of the necessary technical skills […] to ensure the quality and security of the data shared" is ensured.[248] A study among German undertakings shows the importance of sufficient skills as well. In total, more than 47% of questioned companies, stating their implicit willingness to exchange data, declared that a lack of expertise acts as a barrier for them to do so.[249]

3.4 Data localisation requirements for personal and non-personal data

As described above, the EU Regulation for the Free Flow of non-personal data provides the legal framework that allows for the free flow of non-personal data within the EU. It expressly addresses data localisation requirements within the EU for grounds of public security only.[250]

Regarding personal data, the GDPR provides for the free movement of personal data within the EU and specifies that this free movement "cannot be restricted nor prohibited for reasons connected with the protection of natural persons with regard to processing of personal data".[251]

If a Member State imposes localisation requirements on personal data other than for the protection of personal data – e.g. for regulatory control by tax authorities, these requirements will be assessed against the provisions on the fundamental freedoms and the permitted derogations in the TFEU and relevant EU legislation.[252]

In any case, data localisation requirements limit the possibility for service providers (esp. cloud service providers) to scale their business in the EU as operating data centres in many Member States

245 Id. p. 94
246 Everis (2018), p. 95
247 Id. p. 77
248 Id. pp. 44 and 45
249 IWConsult (2019), p. 64
250 Article 4 (1), Regulation (EU) 2018/1807.
251 Article 1(3), GDPR.
252 EU-Commission (2019), p. 13.

drives costs. Overall it was estimated that data localisation requirements could cause €52 billion economic losses in the EU.[253]

Hence, data localisation requirements for personal and non-personal data can constitute an obstacle for the realisation of a single market for data in the EU.

4 Secondary data markets: Nine Recommendations

4.1 Personal Data

4.1.1 Consent as the legal basis for an EU market for business data

An EU market for business data would consist of a network of controller-to-controller transactions. In this context, each controller would need to rely on a specific legal basis among the ones listed by Article 6 GDPR for each and every processing operation, be it the disclosure of data by transmission to another controller or the direct use of such data.

The requirement that a specific legal basis must support each personal data processing operation is a legal challenge for the development of a market for datasets (that normally includes personal data). A solution can lie in the identification of one legal basis, among those mentioned by the GDPR, that is able to support multiple processing, i.e. processing operations by the 1st controller and, upon transfer from him, further processing activities by third party subjects.

A viable candidate in this sense is consent.[254] However, its legitimate use for multiple processing requires such processing to serve a unique purpose that the data subject must have expressly approved[255], as originally established by the CJEU in *Deutsche Telekom.*[256]

4.1.1.1 The notion of consent under the GDPR and its legal requirements

The interpretation of consent under Article 6 (1)(a) GDPR must be in line with the fundamental rights-oriented approach of the legislation. This means that, while the importance of control exercised through consent is expressly acknowledged by the current legal framework, the notion must be

253 Bauer M., Ferracane M., Lee-Makiyama H. and van der Marel E. (2016), p. 11.

254 According to Article 6 (1)(a) GDPR processing shall be lawful, *inter alia*, if "the data subject has given consent to the processing of his or her personal data for one or more specific purposes".

255 "In line with the concept of purpose limitation, Article 5(1)(b) and recital 32, consent may cover different operations, as long as these operations serve the same purpose" (ARTICLE 29 WORKING PARTY (2017), p. 12).

256 Judgement of the 5 May 2011, Deutsche Telekom, C-543/09, EU:C:2011:279.
Deutsche Telekom regarded the interpretation of the Directive on privacy and electronic communications [Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) O.J. 2002, L 201/37]. The case was originated by a national dispute triggered by a telephone service undertaking, which was compelled by national law to release the data relating to its subscribers to a third party for the latter to publish them in a public directory. One of the questions referred to the Court was whether, under EU law, Member States could oblige telephone service undertakings to such disclosure even without previously informing their customers and without obtaining their prior consent. In this regards, the Court stated that EU law does not require renewed consent from the subscribers for the passing of the same data to another undertaking in so far as the data in question (i) has already been collected for publication and (ii) will not be used for purposes other than those for which the data were originally collected. According to the Court, the fact that the data subject has already given his consent to the processing of his data for a specific purpose makes further use of the data for the same purpose uncapable of substantively impairing the right to protection of personal data [Judgement of the 5 May 2011, Deutsche Telekom, C-543/09, EU:C:2011:279, para. 66].

construed so as to confer to the individual a substantial – and not merely formal - control over his own data.[257]

This purposive interpretation should equally apply to the characteristics that, according to Article 4 (1)(11) GDPR, consent must possess to be valid for data processing purposes. Under this provision "'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she […] signifies agreement to the processing of personal data relating to him or her".[258] Moreover, such communication must be made "by a statement or by a clear affirmative action".

All this means that, first, the condition that consent must be "freely given"[259] must be read as requiring the data subject to be in the position to truly choose between accepting and refusing data processing. The consent clause under Article 6 (1)(a) GDPR is therefore not applicable, *inter alia*, to cases of imbalance of power between the data subject and the potential data processor.

Such an imbalance typically occurs in the employment context. As clarified in the *Guidelines on consent*[260] by the Article 29 Working Party, "[g]*iven the dependency that results from the employer/employee relationship, it is unlikely that the data subject is able to deny his/her employer consent to data processing without experiencing the fear or real risk of detrimental effects as a result of a refusal.* […] *Therefore, WP29 deems it problematic for employers to process personal data of current or future employees on the basis of consent as it is unlikely to be freely given*".[261] As a consequence, "[f]*or the majority of such data processing at work, the lawful basis cannot and should not be the consent of the employees (Article 6(1)(a)) due to the nature of the relationship between employer and employee*".[262]

This does not mean that situations in which consent can be relied on as a lawful basis for processing are not imaginable in the employment context. In cases where the employee would face no detrimental consequence following denial of consent, consent is deemed to be truly free.[263] The analysis therefore requires a case-by-case assessment.

Secondly, the reference by Article 4 (1)(11) GDPR to data subject's consent needing to be "specific" must be subject to an equally substantial interpretation. According to the *Guidelines on consent,* the specificity condition is only satisfied when: (i) each and every purpose of processing for which consent is asked is specifically mentioned; (ii) the consent request is "granular" (i.e. it allows the data subject to separately consent to different personal data processing operations and/or does not make the performance of a contract dependent on the consent, despite such consent not being necessary for such performance)[264]; (iii) information related to obtaining consent for data processing activities

257 Article 29 Working Party (2017), p. 9
258 Article 4(11) GDPR
259 Article 4 (1)(11) GDPR
260 Article 29 Working Party (2017), p. 7
261 Article 29 Working Party (2017), p. 7
262 Article 29 Working Party (2017), p. 7
263 Example: "A film crew is going to be filming in a certain part of an office. The employer asks all the employees who sit in that area for their consent to be filmed, as they may appear in the background of the video. Those who do not want to be filmed are not penalised in any way but instead are given equivalent desks elsewhere in the building for the duration of the filming" (see ARTICLE 29 WORKING PARTY (2017), p. 7).
264 Recital 43 GDPR

is clearly separated from information about other matters.[265] This rules out the possibility that an EU market of business data can ever be based on broadly framed declarations of consent by the affected data subjects.

Thirdly, the requirements of informed and unambiguous consent must be also read in substantial terms. Consent, in line with the fundamental principle of transparency, is only informed when it enables data subjects "*to make informed decisions, understand what they are agreeing to, and* […] *exercise their right to withdraw their consent*".[266] Accordingly, the data subject whose consent is asked for must have been made aware of those elements that are essential to make a choice.[267]

Most notably, the Article 29 Working Party points out in its Guidelines that in principle consent is only really informed when named. This means that, when consent is used as a legal basis jointly by multiple controllers or for multiple processing operations, i.e. by other controllers than the original recipient of consent, the identity of the additional controllers should be known to the data subject.[268]

As to the formal requirements, Article 7 (2) GDPR prescribes that, when consent is given in the context of a written declaration which also concerns other matters, "*the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language*". Any violation of those provisions deprives the affected part of the declaration of its binding effect.

Concerning the necessary lack of ambiguity that must characterize consent under Article 4 (1)(11) GDPR, the Regulation makes it clear that either a statement or a clear affirmative act is required; "a clear affirmative act" meaning that "the data subject must have taken a deliberate action to consent to the particular processing".[269]

Finally, consistently with the substantial approach to the GDPR, the right to withdraw one's consent under Article 7 (3) GDPR must be read extensively, as a further building block in the construction of a regime of full control over one's own data.

In the light of the above, due to its fundamental rights-oriented approach, the GDPR does not leave room for an extensive understanding of the data subject's consent as a legal basis. Consent can be considered as a promising legal basis for the development of a network of users of data because of its ability to support multiple processing. Substantial constraints derive, however, from the legal requirements for consent to be valid.

Also, in an overwhelming majority of cases an imbalance of power between the employee/data subject and the employer/data processor will prevent the latter from lawfully processing the former's data, so that employees' data is in principle not available for processing based on consent. This might

---

265 This means that "controllers should provide specific information with each separate consent request about the data that are processed for each purpose, in order to make data subjects aware of the impact of the different choices they have. Thus, data subjects are enabled to give specific consent. This issue overlaps with the requirement that controllers must provide clear information" (Article 29 Working Party (2017), p. 11).

266 "If the controller does not provide accessible information, user control becomes illusory and consent will be an invalid basis for processing" (Article 29 Working Party (2017), p. 13).

267 Article 29 Working Party (2017), p. 13

268 Article 29 Working Party (2017), p. 13

269 Article 29 Working Party (2017), p. 16

constitute a relevant obstacle for the establishment of a common market of business data because a lot of such data regards employees.

4.1.1.2 Making the most of consent as a legal basis - The case for Data Trustees.

Consent as a legal basis could enable the data subject to effectively keep control of his data by selecting the purpose(s) of its processing, irrespectively from the number of processing operations. In this sense, consent could be a promising legal basis for enabling processing of personal data across a network of digital economy actors.

By an operational point of view, however, the level of informative effort laying on the controller/undertaking and the level of cognitive fatigue required to the data subject to ensure a genuine co-control of data processing could be perceived as too high and finally hinder the establishment of a market for business data[270]. Notably, reading and appreciating the implications of the data access requests could prove hard for the data subject, so that two equally undesirable scenarios could materialize: either the data subject would provide his consent without a proper understanding of the consequences of his decision, thus undermining the protection granted by the GDPR, or the data subject would deny access independently from the merits of the data access request, as a self-defence mechanism. Those attitudes are both prejudicial to the establishment of a healthy market for data.

This problem could be mitigated through the establishment of data trustees. A data trustee is a Personal Information Management System (PIMS) that (1) exercises data rights on behalf of the data subject[271] and (2) handles data access requests regarding the data subject on behalf of the data subject. It fulfils those tasks according to detailed directions expressed by that data subject himself.[272]

According to this model, the trustee first exercises on behalf of the data subject the latter's portability right, so as to gather the data subject's personal data that are currently under the control of different entities. The first benefit of data trusteeship for the data subject therefore is to put him back in control of a plethora of data regarding him, which is currently dispersed throughout the datasphere.

Secondly, the data subject entrusts the trustee with an exclusive mandate to manage data access requests regarding his personal data. Also, the trustee must be vested with the power to represent the data subject *vis à vis* third parties through an express declaration of the data subject himself.

Following the conclusion of the trusteeship agreement, the data trustee should be able to (i) collect any data access request by any undertaking regarding the data subject's personal data (ii) verify whether the intended use of the personal data matches with the data subject's preferences and (iii) grant access/express denial. The added value of the data trustees' intermediation would lie in its

---

270 To which extent the controllers can be considered as Joint Controllers in the meaning of Art. 26 GDPR is out of the scope of this study.

271 The distinctive feature of the data trust in respect to other models of PIMS is that "the data trustee is a legal entity that receives a mandate from the data subject to exercise data rights on behalf of the data subjects" (Wendehorst (2017), p. 351). Such "data rights" would be "the rights under the GDPR (as well as the upcoming e Privacy Regulation), but also intellectual property rights, such as copyright in user-generated content and to a very limited extent personality rights, as far as these may be made subject to economic transactions" (ibidem). A review of private initiatives offering personal information services in general can be found at EU-Commission (2016). As to public initiatives to promote the establishment of PIMS, see Poikola A., Kuikkaniemi K. and Honko H. (2018).

272 The model of data trustee hereby proposed is the one described by Wendehorst (2017), p. 349 – 350.

professional character. This entails that the data subject must express his preferences as to the possible uses of his personal data at a very granular level. In this scenario, the trustee is ideally a mere data processor of the data subject.

It should be added that data trustees could have an additional function to data protection, which, while not strictly relevant for the matter under discussion (i.e. how to integrate mixed datasets of personal and non-personal data within the Big Data economy), could prove crucial for their success. Notably, when it comes to evaluating the consumer/data subject' data in the context of an on-line transaction, data trustees could be used to neutralise the asymmetry between the negotiating positions of, on the one hand, the consumers/data subjects and, on the other, the undertaking/controller. They would, in other terms, address the issue of consumers underestimating their data and providing consent "*without having been promised a valuable counter-performance*".[273] In this scenario, it is not data protection which comes into consideration but consumers' protection.[274]

4.1.2 Recommendation No. 1: Making the most out of consent as a legal basis - Data Trustees in practical terms

Most national legal orders supposedly allow the undertaking of a data trustee business as of today, based on rather traditional private law tools.

However, a report drafted by the Commission in 2016 identified substantial obstacles for the data trusts' establishment on the market.[275] Those are:

- the "culture of the provision of "free" services for individuals over the internet", which prevents – especially the least skilled consumers - from grasping the added value of a data trustee;
- the obvious lack of trust of consumers and companies in new entrants, which is particularly serious for businesses aiming to undertake such a trust intensive activity.[276]

Those fundamental issues affecting the consumers' perception of data trusteeship produce huge repercussions on the other side of the market, i.e. vis à vis companies willing to use the data provided by the data trustees in compliance with the data subjects' indications. Entering an agreement with one or more data trustees can only be attractive for data-hungry businesses in so far as the data pools they can access are sufficiently deep. Consumers' mistrust/lack of understanding thus makes the very establishment of this market hard if not impossible.

Recommendation No. 1

The Commission should keep on monitoring closely the evolution of the market of data trusteeship to timely detect the emergence of any future obstacle preventing the business from going cross border.

Finally, it should be noted that data trusts do not inherently guarantee a good governance of personal data trading. On the contrary, having multiple data subjects entrusting a body with the task to

273 Langhanke C., Schmidt-Kessel M. (2015), p. 219.
274 Id., p. 219.
275 EU-Commission (2016)
276 EU-Commission (2016)

manage their personal data raises new data protection and data safety concerns.[277] Therefore, while the data trustee-model is a valuable tool to render the data subject's consent meaningful and the trading of mixed datasets less exposed to legal risks, it is but "*one piece of a larger governance puzzle*".[278] Notably, the ability of data trustees to effectively safeguard individuals' control on personal data depends upon the following issues:

- whether data trustees guarantee acceptable standards of diligence and fairness while carrying out their activity;
- whether they are sufficiently transparent;
- whether they act in the best interest of the data subjects;
- whether they use adequate and appropriate human and technical resources;
- whether they have a robust conflict of interest governance in place.

A possible future regulation of data trustees at the EU level should ideally address those wider concerns.

4.1.3 Recommendation No. 2: Review of GDPR: Ensuring legal certainty through a higher degree of harmonisation

Now that the GDPR has been enacted, some shortcomings have become apparent. These shortcomings should be addressed within the upcoming review of the GDPR by the European Commission. In particular, measures must be taken to ensure a harmonised and innovation-friendly approach to personal data protection while allowing digital technologies to flourish in Europe.

4.1.3.1 Avoiding GDPR-induced fragmentation

The GDPR contains several "specification clauses", i.e. provisions leaving a wide margin of manoeuvre to Member States concerning specific aspects of personal data protection. While this enables Member States to adapt the GDPR to the national context, it also leads to divergences which may undermine the level playing field of the internal market.

Specification clauses can be of different kinds. First, Member States may select one of the options offered by the GDPR provision. For example, the GDPR sets as a default rule that, in relation to offers of information society services directly to a child, the processing of the child's personal data based on consent is only lawful if the child is at least 16. Member States may, however, provide by law for a lower age limit, provided that it is equal or above 13.[279]

Secondly, under some GDPR provisions the Member States are entitles to modify the legal regime established by the EU legislature, e.g. by establishing exceptions to GDPR rules. One of such provisions is Article 23 GDPR, which allows Member States to restrict the rights of the data subjects when necessary to protect exhaustively enumerated objectives of general public interest, "the protection of the data subject or the rights and freedoms of others" and the enforcement of civil law claims.

Finally, there are cases where Member States are required to "implement" the GDPR, for example by establishing the DPAs in compliance with the minimum harmonisation rules under Chapter VI GDPR.

277 EU-Commission (2016)

278 Wylie B., McDonald S. (2018)

279 Article 8 (1) GDPR. The option may even consist in extending the scope of the GDPR provisions. This is, for example, the case of the obligation to designate a Data Protection Officer (DPO), which might be extended to other cases except the ones listed by the GDPR in Article 37 (1) GDPR [Article 37 (4) GDPR].

Even though the aim of the specification clauses is to grant a differentiated adaptation of the GDPR legal regime within the single national legal orders, their effect could be a substantial lack of homogeneity of the data protection regimes throughout the EU. This could, in turn, disrupt internal market integration[280] and, more specifically, the establishment of an EU market for data.

Given that the very adoption of the GDPR was prompted by the inability of the former legal regime (i.e. the 1995 Data Protection Directive[281]) to achieve a sufficient level of harmonisation of national laws[282], it is advisable that the most problematic provisions are amended. For example, it should be possible to tear down the specification clause allowing Member States to modify the minimum age to provide consent so as to have a single rule on such an important topic.

4.1.3.2 Increasing legal certainty

The complexity and sensitiveness of the matters addressed by the GDPR has led to differences in its interpretation at the national level. There is a need for a more harmonised, EU-wide approach on the following issues in particular:

- the concept of "scientific research purpose" under Article 89 (2) GDPR. This provision enables the EU and national law to provide for derogations to specific data subjects' rights[283] when such rights make it impossible or "seriously impair" the achievement of a specific research purpose. Given the relevance of the topic for promoting breakthrough innovation, a more intense dialogue between data protection authorities in this regard should be launched[284];
- the criteria for controllers to qualify a joint controllers;
- the notions of pseudonymisation and anonymization of data.

Recommendation No. 2

The European Commission should use the upcoming review of the GDPR to ensure legal certainty through a higher level of harmonisation.

4.1.4 Recommendation No. 3: Regulatory sandboxes – creating legal certainty in a market-neutral manner

4.1.4.1 The principle of legal certainty

The principle of legal certainty – which is one of the general principles of European Union law – requires that rules of law be clear and precise and predictable in their effect, so that interested parties can ascertain their position in situations and legal relationships governed by European Union law.[285]

Legal certainty is especially important when referred to rules that are liable to entail financial consequences, in order that those concerned may know precisely the extent of the obligations which those

280 Report "Contribution from the multi stakeholder expert group to the stock-taking exercise of June 2019 on one year of GDPR application", 13 June 2019, p. 21. Korff D. and Georges M. (2019), pp. 55 ff.

281 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (O.J. 1995, L 281/31)

282 Korff D. and Georges M. (2019), pp. 55 ff.

283 Right of access by the data subject (Article 15 GDPR); right to rectification (Article 16 GDPR); right to restriction of processing (Article 18 GDPR); right to object (Article 21 GDPR).

284 European Data Protection Supervisor (2020)

285 See, to that effect, judgement of 27 November 2018, Mouvement pour une Europe des nations et des libertés v Parliament, T-829/16, EU:T:2018:840, point 68 and the case-law thereby cited.

rules impose on them.[286] This applies to the provisions of the GDPR, whose non-observance leads to the application of (very high) sanctions.[287]

Legal certainty also increases efficiency, as it facilitates compliance by those who are subject to the regulation as well as the compliance review by the competent authority.

In this sense, legal certainty should be a guiding value and a primary concern for DPAs, considering the complexity of the GDPR. While the GDPR builds up on the *acquis* of the previous EU data protection framework[288], it brought about important changes. This is the case, for example, for accountability obligations, which are stretched across the whole personal data processing cycle and embody a substantial approach to the responsibilities lying on the various actors involved, whether they qualify as controllers or processors. While this promotes a more realistic match between the level of involvement in the processing and the attached responsibilities, it also blurs the boundaries between the role of data controller and data processor and brings about additional legal risks.[289]

Legal certainty should be mainly promoted through the issuance of guidelines as to how to interpret the GDPR's requirements. Such guidance should ideally be elaborated within the EDPB[290]to ensure a level playing field across the internal market. This is all the more necessary as this was precisely one of the aims of the EU legislature.[291]

The UK's Information Commissioner's Office (ICO) has recently launched a different initiative to promote legal certainty. It has established a regulatory sandbox regarding the application of the personal data protection regulation (including the GDPR) to companies marketing innovative products and services, to "*enhance data protection and support innovation*".[292] In what follows, we will illustrate the initiative and assess whether it is legitimate and appropriate to use the regulatory sandbox model in the area of personal data protection.

4.1.4.2 The ICO's initiative: the essentials

The ICO describes its sandbox as "*a new service designed to support organisations using personal data to develop products and services that are innovative and have demonstrable public benefit*".[293]

---

286 See judgement of the 17 May 2018, Bayer CropScience v Commission, T-429/13 and T-451/13, EU:T:2018:280, points 285, 286 and the case-law thereby cited.

287 See Article 83 para. 4 and 5 GDPR

288 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (O.J. 1995, L 119/1)

289 The CJEU has repeatedly dealt with this issue recently. See, in particular, judgement of the 5 June 2018, Wirtschaftsakademie Schleswig-Holstein, C-210/16, EU:C:2018:388, points 38-39; judgement of 10 July 2018, Jehovan todistajat, C-25/17, EU:C:2018:551, points 68, 72, 73; judgement of 29 July 2019, Fashion ID, C-40/17, EU:C:2019:629, points 74 – 76.

290 Article 70 GDPR

291 "The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data. This Regulation is intended to contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, **to the strengthening and the convergence of the economies within the internal market**, and to the well-being of natural persons" (Considerandum n. 2, GDPR).

292 Information Commissioner's Office (2019), ICO opens Sandbox beta phase to enhance data protection and support innovation, press statement, 29 March 2019, accessible at https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/03/ico-opens-sandbox-beta-phase-to-enhance-data-protection-and-support-innovation/

293 Id.

Access to the sandbox is only granted to a limited number of organisations that are selected through a formal procedure "*on the basis of whether the product or service being developed is innovative and can provide a potential demonstrable benefit to the public*".[294] Notably, "[p]*ublic benefit will be determined in terms of both breadth – the amount of people benefitting – and depth – the extent to which they benefit*".[295]

The service consists in providing "*feedback, steers, guidance, any exit report or document or other advice*"[296] concerning the participating organisation's handling of personal data in reference to a specific innovative product or service.[297] The terms of the relationship between each participant and the ICO must be agreed upon through the "Sandbox Plan", "*which may specify testing parameters, measures for outcomes, reporting requirements, safeguards, timescale and term of the sandbox*".[298]

It must be underlined that the participating organization remains responsible for its compliance with all applicable legal rules[299]. This means, on the one hand, that the participant is free not to follow the ICO's indication[300] and, on the other, that the feedback provided by the ICO does not qualify as a final commitment of the agency.[301]

Finally, the ICO intends to use the sandbox as a means to improve its knowledge of the business context by using the information it gathers (confidential information included) "*to help develop and provide guidance, policies and resources (on an anonymised basis) to the public*".[302]

4.1.4.3 What is a regulatory sandbox?

While the ICO defines its initiative as a regulatory sandbox, there is no common understanding of what a regulatory sandbox actually is.

The model, which was developed in the Fintech context, has been described as a safe space where tightly tailored derogations from specific regulatory requirements are granted to the entities that meet the entry tests, all under the monitoring of the competent authority.[303] This clearly distin-

294 Id., See criteria indicators at https://ico.org.uk/media/for-organisations/documents/2614572/sandbox-criteria-indicators-201903.pdf

295 Id.

296 Information Commissioner's Office (2019), Sandbox Terms and Conditions, March 2019, para. 1.3., accessible at https://ico.org.uk/media/for-organisations/documents/2614577/sandbox-t-c-201903.pdf

297 Id., para. 1.2.

298 Id., para. 4.2.

299 Id., para. 1.6.

300 Id., para. 1.7.

301 "Being accepted into the sandbox does not prevent regulatory action by us or by any other competent data protection authority or by any other regulatory body or authority. The Feedback does not affect rights conferred on third parties (such as your customers), nor does it bind any courts, and may not reflect the views of the European Data Protection Board or any other data protection authority" (Information Commissioner's Office, Sandbox Terms and Conditions, March 2019, para. 1.10., accessible at https://ico.org.uk/media/for-organisations/documents/2614577/sandbox-t-c-201903.pdf). "Any Feedback is given without prejudice to any decision or action that we may take in the future, including any enforcement or other regulatory action. The positions reflected in the Feedback may change over time, for example on receipt of further information us, or following a change in law, court judgments, regulatory guidance or ICO policy" (INFORMATION COMMISSIONER'S OFFICE, Sandbox Terms and Conditions, March 2019, para. 1.10., accessible at https://ico.org.uk/media/for-organisations/documents/2614577/sandbox-t-c-201903.pdf).

302 Id., para. 7.3.

303 Barbagallo C. (2019), Fintech: Ruolo dell'Autorità di Vigilanza in un mercato che cambia, speech held at Convegno invernale dell'Associazione dei docenti di economia degli intermediari e dei mercati finanziari e finanza d'impresa, Naples, p. 11.

guishes the regulatory sandbox from the innovation hub, which is merely a portal connecting the regulators with the entities affected by regulation and which allows the latter to receive in a more efficient and organised fashion clarifications and guidelines as to the applicable legal framework.[304]

This definition of regulatory sandbox would arguably be extraneous to the constitutional tradition of many Member States: indeed, it implies that the competent authority can dispose of the law to better adapt the legal framework to the specific case in front of it, while the principle of legality requires such authority to merely apply the law, as large as its discretion in this respect might be.

Besides, EU law openly prevents the use of such a regulatory model in cases where, as in the personal data protection framework, national authorities are entrusted with the task of applying EU law. The disapplication of relevant EU provisions within the sandbox context would indeed undermine the primacy of EU law and expose the relevant Member State to an infringement procedure.

This is the reason why the report on FinTech issued by the European Supervisory Authorities' (ESA) defines sandboxes as a model providing "*a scheme to enable firms to test, pursuant to a specific testing plan agreed and monitored by a dedicated function of the competent authority, innovative financial products, financial services or business models*" and clarifies that "*sandboxes do not entail the disapplication of regulatory requirements that must be applied as a result of EU law*".[305]

As a consequence, in the EU context the difference between the regulatory sandbox and the innovation hub is less striking: while the former offers a "*scheme*", thus entailing a separate legal environment where the authorities and the organisations interact according to a pre-established set of rules, the latter is meant to provide "*a dedicated point of contact for firms to raise enquiries with competent authorities* […] *and to seek non-binding guidance on the conformity of innovative financial products, financial services or business models with licensing or registration requirements and regulatory and supervisory expectations*".[306] In other terms, absent the possibility for the authority to grant waivers from the existing legal requirements, the element of differentiation lies in the openness of the regulatory model to all market actors.

In this sense, the ICO's initiative can be defined as a regulatory sandbox *à l'européenne*. The object of the following paragraph will be to assess whether it actually is an appropriate tool to improve legal certainty in the area of personal data protection.

4.1.4.4 The ICO's initiative: a model to export?

The ICO's initiative confirms the innovation-friendly approach brought about by the British authority and draws attention to the importance of finding an optimal balance between effective personal data protection and technological development. However, it is not entirely convincing.

First, the fact that the regulatory model at hand is designed to create a closed environment is rather problematic as it fragments the market. There is a serious risk that the advantages of the sand box materialise primarily for the participants. If this were the case, competition between participants and non-participants of the sand box may be distorted. The ICO seems to anticipate this by stressing that the sandbox will be used to improve its knowledge and "*to help develop and provide guidance, poli-*

304 Id.
305 European Supervisory Authorities (2018), p. 5
306 Id.

cies and resources (on an anonymised basis) to the public" .[307] It is however difficult to imagine how such non-exclusive guidance may be given in such a timely matter as to prevent an unlevel playing field.

Secondly, it is at least questionable whether DPAs can promote innovation *per se*. It may well be that the development or offering of highly innovative products or services is impaired by the legal uncertainty surrounding the application of the personal data protection framework. Any initiative by the competent DPA designed to improve legal certainty is entirely consistent with its institutional mandate, which is "*monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union*".[308] Indeed, a more efficient application of the GDPR supports those objectives.

However, ICO's criteria for access to the sandbox suggest that it is not legal clarity (and, therefore, a more efficient application of the GDPR) that the DPA aims to promote, but innovation. Whether access of the selected organisations to the sandbox will provide an added value regarding the enforcement of the personal data protection legal framework does not seem to be a primary concern to the ICO.

Recommendation No. 3

Initiatives that aim at increasing legal clarity by establishing a dialogue between Data Protection Authorities (DPAs) and businesses or innovators are to be supported. They can help DPAs to identify new developments in technology and innovation while ensuring that people's rights to privacy and data protection are respected. At the same time, these initiatives, whether called "sandboxes" or "regulatory hubs", must be market neutral (i.e. available to all market participants) and genuinely devoted to improving legal certainty in the application of the personal data protection framework.

4.2 Public sector data

The 2019 review of the PSI Directive addressed a number of obstacles to the availability of data from public sector entities. The following recommendations highlight room for action by the European Commission in order to promote the access and re-use of public sector data.

4.2.1 Recommendation No. 4: More standardisation

Without standardised formats, each public sector body in the Member States can make data available in different formats, thus making re-use more expensive. The development of uniform sectoral open standards is therefore needed to ease access and further increase the re-usability of public sector data. Notably, standards are needed for data exchanges, for document handling and for IT security. Also, the establishment of harmonised sectoral platforms can facilitate access and re-use of data.

---

307 Information Commissioner's Office (2019), Sandbox Terms and Conditions, March 2019, para. 7.3, accessible at https://ico.org.uk/media/for-organisations/documents/2614577/sandbox-t-c-201903.pdf

308 Article 51, para. 1 GRPR

Recommendation No. 4

The Commission should develop, together with the relevant stakeholders, open standards on platforms and data formats for public sector bodies to make data available. The standardisation should be carried out on a sectoral basis.

4.2.2 Recommendation No. 5: Availability of privately held data in the context of the provision of public interest services and public procurement

The public entities that have to make their data easily re-usable after the 2019 review of the PSI Directive are:

- Public sector bodies – i.e. State, regional or local authorities;
- Bodies governed by public law – i.e. bodies which are established for the specific purpose of a general interest need (and not having an industrial or a commercial character), have legal personality, and are financed or subject to management supervision by public authorities or other bodies governed by public law, or have more than half of the members of their administrative, managerial or supervisory board appointed by such bodies;
- Public undertakings – i.e. companies active in the areas of water, energy, postal services, or public, maritime or air transport, over which public sector bodies have a dominant influence.

Private companies are not covered by these obligations regarding re-use of data. However, public authorities may entrust the provision of services of general economic interest (SGEI), such as postal services and public transport, to private sector companies. Extending the scope of the Directive to such companies would increase the opportunities for innovation by having a larger amount of data available for re-use.

It would be useful to include private companies providing SGEI in the scope of the PSI Directive to have privately held data of public interest available for various re-users. However, an obligation to make such data available for re-use shall be precisely defined and shall include:

- A definition of the type of data concerned, i.e. the data relating to the provision of the service and that is not linked to a company's know-how;
- Safeguards of the legitimate commercial interests of private companies, especially restrictions on access and re-use due to the protection of trade secrets and intellectual property rights, as well as personal data protection and security safeguards;
- A clear definition of the notion of "public interest" which shall relate to its objective (e.g. the provision of gas and electricity) and might be based on a sectoral approach.[309]

Furthermore, public sector entities should also make use of the opportunities they have to access and then open up data generated by private companies in the framework of public procurement. This could be done by conditioning the purchase of works, goods and services by public authorities to the availability for use of the data generated by the private companies in this context, while ensuring restrictions on trade secrets and data protection.[310] Once public sector entities have access to this data, they could make it available to third-parties.

309 E3PO, Comments on the review of the PSI Directive – Public consultation, 12th December 2017.

310 Bundesministerium für Wirtschaft und Energie (2019a), p. 47

Recommendation No. 5

The Commission should extend the scope of the PSI Directive to include private companies providing public interest services, thus ensuring the availability of privately held data relating to the provision of the public interest service. The Commission should also encourage Member States and their public authorities to make public procurements conditional upon the availability of the data generated in this context.

4.2.3 Recommendation No. 6: Investigate the need for an access right for high value datasets

The PSI Directive does not impose on Member States a general obligation to make public sector data available to the public. Instead, it sets out a number of requirements that public sector bodies and undertakings have to comply with, with the view of ensuring that such entities make that data, which is already available to the public, also available for re-use. The PSI Directive thus ensures minimum harmonisation of national rules on the re-use of public sector information. Its aim is to facilitate such re-use.

There are discussions on the idea to establish an obligation to grant access to public sector data and private data of public interest. On the one hand, this would grant market operators the opportunity to create innovative products and services through the use of this data while, at the same time, ensuring a level playing field for all players – whether private or public. This is especially important for high value datasets – i.e. geospatial, earth observation and environment, meteorological, statistics, companies and mobility data.

On the other hand, an obligation to grant access implies higher costs to be carried by public entities and private companies providing a public interest and risks resulting in competition distortions. Furthermore, there is no one size fits all principle, the advisability of such an access obligation very much depends on the sector and the business models concerned. The opponents to an access obligation generally also argue that voluntary agreements are sufficient to ensure fair access to data.

For example, while the French national rail company SNCF is not in favour of freely sharing the data it holds with private competitors because it wants to safeguard its commercial interests and sees a risk of competition distortions, the European digital train platform Trainline wants fair access to be ensured for all players in the sector because rail data is necessary for the services it offers.[311]

Recommendation No. 6

The Commission should investigate whether establishing a general obligation to grant access to public sector data and public interest data might be necessary, first and foremost for high-value datasets. It should especially look into the existing data sharing practices of public and private companies in particular sectors – e.g. transport, geospatial – to evaluate if data sharing based on voluntary agreements is sufficient or if further action – be it through soft-law measures or binding EU law – is required.

311 See the position papers received in the framework of the 2017 public consultation on the review of the Directive 2003/98/EC on the re-use of public sector information of the SNCF and of Trainline, available at: https://ec.europa.eu/digital-single-market/en/news/additional-position-papers-sent-framework-consultation-review-public-sector-information

4.3 Non-personal data

4.3.1 Recommendation No 7: Promote B2B Data Sharing through European data spaces

On 24 April 2018, the European Commission adopted the Communication "Towards a common European data space".[312] Common data spaces should provide a trusted framework to facilitate access to and subsequent use of privately held data and to promote B2B data sharing in specific and between sectors.

The Commission has already organised workshops with relevant stakeholders from various industries – such as finance, agriculture, health and energy – to discuss the common understanding of the business potential, the obstacles and common measures to advance B2B data sharing.[313]

In order to operationalise the common European data spaces, the Commission propose to foresee funding for such data spaces as of 2021 under the new 'Digital Europe Programme'.[314]

The EU data space initiative could be instrumental to address some of the concerns and obstacles – that were outlined above – that hamper B2B data sharing in Europe. By bringing together the relevant private and public actors and pooling knowledge and expertise, the sectoral spaces can reduce transaction costs for both data sellers and buyers. The initiative could for example facilitate the development of industry data platforms, technical standards or templates for contractual terms and conditions for B2B data sharing.

It should be stressed that all public action should be market neutral and not impede the level playing field.

Recommendation No. 7

The European Commission's European data space initiative may contribute to reducing transaction costs of B2B data sharing in Europe. The initiative deserves to be intensified as long as it is market-neutral by design.

4.3.2 Recommendation No. 8: No need for a data property right

Establishing a property right in data consists of conferring exclusive rights in non-personal data - especially the right to use, to exclude access and to transfer - upon natural or legal persons that produce the data. Compared to exclusive property rights in material goods, the special characteristics of data, such as their intangible or non-rival nature, make it more difficult to define who owns the data as well as to prevent data access and use.

Various reasons can justify the need to define a property right in data. The main justification is to create an incentive to produce data. An incentive problem arises when there is non-rivalry and non-excludability in the use of data and non-excludability, thus creating a risk that the data producer lacks sufficient incentive to collect, produce and analyse data because others could copy its innovation.[315] Conferring exclusive rights upon data producers is thus expected to encourage him to do so.

312 EU-Commission (2018a)
313 EU-Commission (2019e).
314 EU-Commission (2019e), p. 1
315 Kerber, W. (2016), p. 8-9.

Data ownership is also seen as a mean to stabilise and facilitate transactions in data - contrary to factual exclusivity, which does not ensure direct remedies *vis à vis* third persons using the data without any authorisation.[316] Another argument for the establishment of a data property right is that it enhances legal certainty by clearly fixing the rights and obligations of the different stakeholders. Finally, a property rights regime could enhance access to data if it includes exceptions and limitations, ensuring a greater access than relying on contract law and the underlying principle of freedom of contract.[317]

Currently, the EU legal framework - which is composed of the Database Directive, the Trade Secrets Protection Directive and the GDPR - only provides for partial and limited ownership rights on data.

The Database Directive[318] gives (i) full copyright protection to original databases – i.e. databases that are the result of a creative human effort – and (ii) a "sui generis" database protection for non-original databases where "there has been a qualitatively and/or quantitatively substantial investment in either the obtaining, verification, or presentation of the contents".[319] The "sui generis" protection is, however, very limited. It does not apply to the contents of the database – i.e. to the data itself – but to the structure – i.e. the database as a whole[320]. The CJEU contributing in limiting the scope of the sui generis right by narrowly interpreting the substantial investment requirements: according to the Court, it relates to the resources used to seek out and collect materials in the database and not to the resources used for the creation of the data.[321]

The second relevant regime regarding data ownership is trade secrets. While the Database Directive only protects the structure of the data and not the individual data comprised in it, trade secrets protection has the potential to do so. However, the Trade Secrets Directive[322] remains rather unclear regarding the protection of data produced by smart products and provides for narrow requirements. Trade secrets protection in the framework of the Directive does not consist of a property rights regime, but rather of a liability system for specific tortious conduct – i.e. the unlawful acquisition, use and disclosure of trade secrets.[323]

Finally, the GDPR recognises a certain number of rights to individuals regarding their personal data. The rights vested in the data subject over their personal data do not however equal to full and tradable ownership rights, because personal data protection is a basic and inalienable fundamental right that may not be traded away.[324] Thus, individuals have control rights over their personal data, not property rights.

In the light of the above, data ownership is currently a *de facto* right: the ownership rights on data come from the factual control over data.[325] Despite the non-existence of a general data property

316 Drexl (2017), p. 275.
317 Id., p. 275-276.
318 Directive 96/9/EC of 11 March 1996 on the legal protection of databases.
319 Art. 7(1), Database Directive
320 Art. 3(2), Database Directive
321 Judgement of 9 November 2004, British Horseracing Board, C-203/02, ECLI:EU:C:2004:128, para. 31.
322 Directive (EU) 2016/943 of the European Parliament and the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets), use or disclosure.
323 Drexl (2017), p. 269.
324 Duch-Brown, N., Martens B. and Mueller-Langer F. (2017), p. 16.
325 Id. p. 18.

right, businesses are able – by factually controlling the data – to exclude others from accessing the data, especially through technological protection measures (e.g. encryption).

Contract law is also an important tool for data holders to prevent others from using their data. The factual holding of data allows data producers to conclude agreements that restrict access and use of data.[326] The limits of contract law in regulating data access and use concern third parties – i.e. not signatories to the contract: the data holder has no legal means to enforce his rights or remedies against their unauthorised use of data.[327]

Considering the justifications for a data property right, the incomplete EU legal framework on data ownership and the loopholes that characterise contract law when it comes to the protection for the data producer, there is a debate on the need (or lack of) to create a legal ownership right on data. This question was also raised on a public consultation from the Commission[328]. In that context, respondents mainly rejected regulatory intervention by the Commission to establish data ownership rights for the data producer and/or manufacturer.

The opposition to the establishment of exclusive property rights on data can first and foremost be explained by the weakness of the incentive argument. There is indeed little evidence that data producers are lacking incentives to collect, produce and analyse data in the current situation, as shown e.g. by the massive production of data in the context of Big Data.[329] More importantly, data producers have the means to exclude, i.e. to protect their data against access and use by third parties, through technological protection measures and contractual arrangements. Without an ownership right, data producers can therefore already protect their innovation against copying.

Furthermore, if it was to be introduced, the design of a data property right would prove to be difficult. Challenges are especially linked to the definition of the subject-matter of protection (definition of data, determination of the owners of the data property right, identification of an appropriate scope of protection)[330]. These practical problems would likely cause legal uncertainty. Another challenge in the creation of an ownership right in data is the need to maintain a balance between property rights and the public interests whose fulfilment requires access to and use of data – e.g. to foster innovation, support research and education. Also, there is no one-size-fits-all approach on data ownership considering the variety of business models and data. An ownership right in data would offer at the end less flexibility for businesses than regulating access through contract law and could therefore negatively impact the free flow of data.

All in all, we consider the arguments brought forward in favour of creating a data ownership right not convincing, especially the incentive and the legal certainty arguments. Moreover, introducing such a right would entail a certain number of disadvantages and challenges. *De facto* control over data and the elements currently available to data producers to regulate data access – contract law and technical restrictions – form a sufficient basis for data market development.

326 Drexl (2017), p. 272.
327 Duch-Brown, N., Martens B. and Mueller-Langer F. (2017), p. 15; Drexl (2017), p. 275.
328 Public consultation on Building the European Data Economy.
329 Kerber (2016), p. 8-9.
330 Drexl (2017), p. 277.

Recommendation No. 8

A legal ownership right to data should not be introduced. De facto control over data through contract law and technical restrictions form a sufficient basis for data market development.

4.3.3. Recommendation No. 9: Address unjustified data localisation requirements

As described before, the FFD-Regulation and the GDPR set out a legal framework for data localisation requirements relating to personal, non-personal and mixed data sets. Member States' possibilities to introduce data localisations requirements are restricted and the degree of that restrictions depends upon the nature of the data.

Regarding non-personal data, the FFD-Regulation expects data localisation requirements – except for reasons of national security and when proportional – to be lifted by May 2021. As such localisation requirements hinder the development of a single market for data in the EU, the Commission should closely monitor the lifting of any remaining requirements and swiftly act against Member States which do not adhere to the FFD-Regulation.

Regarding personal and mixed data, data localisations requirements are generally allowed if compatible with the provisions on the fundamental freedoms and the permitted grounds to derogate from those freedoms emanating from the Treaties[331] and not based upon data protection considerations. Here as well, the Commission should consistently proceed against any data localisation requirements that are not compatible with the EU-Treaty provisions.

Recommendation No. 9

As data localisation requirements hinder the development of a single market for data in the EU, the EU-Commission should consistently proceed against national data localisation requirements that are not justified under the GDPR and the FFD-Regulation. In order to enable the identification of data localisation requirements under the GDPR, the possibility of installing a register for national data localisation requirements under the GDPR should be investigated.

331 EU-Commission (2019), p. 13

CHAPTER III: PRIORITY 2 - MAINTAINING EFFECTIVE COMPETITION

This chapter sets out very briefly in section 0 the relevance of platforms and data to competition in the digital economy. In section 2, we deal with a selection of competition issues we believe to be of particular relevance to the digital economy. We first focus (in section 2.1) on abusive behaviour related to access to infrastructure and data. In section 2.2 we deal with anti-competitive agreements related to sharing data. We offer five recommendations.

The mentioned competitive issues are described by certain problem cases. These cases are not an exhaustive list but describe issues for various offerings in the relevant cloud offering areas.

1 The digital economy: Key factors of relevance to competition

The digital economy's platform character has serious implications regarding the level of competition in the sector. We first deal with market power on platforms before explaining the role of data.[332] Some of the basics of platform economics have already been dealt with in chapter I.

1.1 Platforms and Market Power

In order to determine the market power of a platform one has to determine the relevant market in the first place. To determine whether a product or geographical region is part of the relevant market one has to look at substitution in supply or demand. Usually the SSNIP-Test is used to determine the relevant market. In the case of a multi-sided platform the result can be misleading for three reasons:

- The SSNIP-Test takes into account only changes in supply or demand on one side of the platform. On a multi-sided platform, an increase in the price for one group can have an effect on the other group. Hence, determining the relevant market is possible only when taking into account these effects on all sides of the platform.[333]

- The SSNIP-test can be conducted only when positive prices exist. However, a number of platforms in the B2C digital economy do not charge users on one side of the platform, for instance due to high price sensitivity. An increase in the price by 5 to 10% using the SSNIP-test can hence not be simulated.

- The SSNIP-Text is static; it may not be able to sufficiently cope with blurring and constantly changing boundaries of the different markets.[334]

Once the relevant market has been determined, the market power of a platform should be examined. According to the European Commission, an undertaking has a significant market power if it is able "to prevent effective competition being maintained on a relevant market, by affording it the power to behave to an appreciable extent independently of its competitors, its customers and ultimately of consumers".[335] This is usually the case if an undertaking is able to raise the price above

---

332 This part draws upon the cepStudy, Competition Challenges in the Consumer Internet Industry, February 2016; available at: https://www.cep.eu/eu-themen/details/cep/competition-challenges-in-the-consumer-internet-industry.html

333 Filistrucchi L. (2008)

334 Van Gorp and Batura (2015), p. 52.

335 European Commission (2009), p. 7

marginal costs.[336] In the case of platforms however, this could be misleading. Due to the different price structure for user groups, a high price for one user group is not necessarily a sign for a significant market power. It might be necessary in order to attract another, price sensitive user group in the first place.

The same applies to the calculation of market shares. A platform can have a considerable market share on one side of the platform. This does however not suffice to conclude that the platform has a significant market power, because on the other side of the platform it might have only a relatively small market share.[337] Hence, one has to take into account all sides of the platform as well as the indirect externalities in order to determine the market power of a platform.

At the moment, there is no standard method for analysing market power on two (or more) sided markets.[338] The SSNIP-test is being adapted, in an attempt to take account of the mentioned problems and incorporate repercussions on total profitability of the firm or on the demand elasticity.[339] Van Gorp and Batura propose an alternative path. Instead of primarily searching for potential substitutes for a product to define the relevant market, they suggest taking a closer look at “business models”. Especially, the way how dominant companies of the consumer internet industry “generate turnover and profit” and whom they “steal away profits” ought to be focused.[340]

1.2 Data as an input- and output-factor

In a number of markets of the digital economy, data may be decisive in order to be able to offer a competitive service. When such data is available to only a few enterprises or available to others only at costs exceeding those of competitors, fair competition may be hindered. In economic terms, data may be a “bottleneck". In legal terms, we speak of an “essential facility".

In most cases, data may be only one of many factors contributing to service providers being able to gain a dominant position on any given market. By no means, must data be the sole or most important one. Also, the degree of data being a bottleneck for competition may vary, as substitutes to data may be available (at a cost). However, depending on the case, it may be a decisive bottleneck.

At the same time, the availability of data – or the lack thereof – may strengthen existing competition constraints. This is so as data may both serve as a relevant

- input-factor to a given service (increasing its quality and hence offering a competitive advantage); but also as an
- output of the offering of exactly this service. This may aggravate the competition problem, as the output-data can be re-used as an input to this service – or other services in adjacent markets – and may improve it, furthering competitive advantages at the expense of the entity having no data access.

336 Evans D. (2009), p. 35.
337 Monopolkommission (2014), paragraph 56.
338 Dewenter, R. and Rösch J. and Terschüren A. (2014)
339 Filistrucchi (2008).
340 Van Gorp and Batura (2015), p. 56.

2 Competition issues in the digital economy: Five Recommendations

In the following, we focus on competition challenges in the digital economy related to the abuse of market power (in section 2.1) and anti-competitive agreements (in section 2.2). Clearly this is only a subset of potential competition issues. The challenges related to mergers and acquisitions may be very relevant as well, but are already well documented.[341]

2.1 Abusive behaviour regarding access to infrastructure and data

European competition law practice generally provides for five types of actions, which are seen as abuses of a dominant market position.[342] The problems we will discuss relate to the following two types of actions.[343]

- **Actions limiting production, markets or technical development**[344] form the bulk of inadmissible behaviour. They cover typical monopolistic behaviour of suboptimal low output in combination with sub optimally high prices. Given that proving such behaviour is possible only in exceptional cases, competition practice has focussed on enterprises limiting sales, production or access to inputs vis-à-vis other market participants. This type of behaviour by the market dominant enterprise may limit or prohibit production by competitors.
- **Tying**[345] is given where customers buying one product (the tying product) from an undertaking with a dominant position on the market for that product must also buy another product (the tied product).[346] The tying can take place on a technical or contractual basis.[347] **Bundling** refers to the way products are offered and priced by a dominant undertaking and can take two forms:[348] Pure bundling is given where products are only sold jointly in fixed proportions.[349] Mixed bundling, often referred to as a multi-product rebate, is given where products can also be bought separately, but the sum of their prices is higher than the bundled price.[350]

In the following, we will deal with four different problem cases. Problem case 1 -3 deal with infrastructure as a factor that may hinder effective competition. Problem case 1-2 relate to actions limiting production, markets or technical development; whereas problem case 3 also relates to tying and bundling. Problem case 4 relates to data as a crucial factor for competition. Problem case 3 and 4 deal with vertically integrated enterprises.

2.1.1 Problem case 1: Abusive behaviour on the IaaS-Market (Hyperscalers)

2.1.1.1 Description of the problem

The market for large scale cloud service providers (hyperscalers) is currently characterised by intense competition and a high level of innovation, but at same time by a significant concentration of the market. However, as the hyperscaler cloud market is confronted with high fixed costs, the number of

341 Cf. Bundesministerium für Wirtschaft und Energie (2019a) (Chapter VIII) or Crémer J., de Montjoye Y., Schweizer H., (2019) (Chapter 6)
342 Art. 102 (2) TFEU.
343 The remaining actions cover discrimination, unfair prices and trading conditions and exclusive dealing.
344 Article 102 (2) (b) TFEU.
345 Article 102 (2) (d) TFEU.
346 European Commission (2009), paragraph 48 in conjunction with footnote 3 to paragraph 50.
347 European Commission (2009), paragraph 48.
348 Ibid.
349 Ibid.
350 Ibid.

successful hyperscale cloud suppliers in the future can be expected to remain very limited (for concentration tendencies, see page 12). This may result in monopolistic prices and terms of use.

The present situation on the cloud market segment for hyperscalers clearly is one of intense competition. All hyperscalers are trying to maximise the degree of utilisation of their infrastructure as this enables them to be competitive on the market.

For this reason, hyperscalers may have an incentive to increase their users' costs of switching providers. High switching costs cause lock-in effects for hyperscaler users, which may increase the degree of infrastructure utilisation.

The effects of high switching costs on consolidation – and hence on the degree of competition – in the hyperscaler market are not clear ex-ante. On the one hand, it may increase users' dependency upon a given provider and hence lower competition. On the other hand, it may slow down or prevent the further consolidation of the market to a very limited of number of providers only. Also, it is common practice amongst business users to parallelly use the service of different hyperscalers (multi-homing) to prevent excessive dependencies and technical risks. Given that there is a demand for using different hyperscalers' infrastructure, switching costs may lower competitive pressure, but the real bottleneck for competition rather seems the very limited number of hyperscalers to which any switching is possible at all.

2.1.1.2 The appropriate policy

2.1.1.2.1 Step 1: The contestability test

From a competition point of view, any public intervention should be strictly made conditional upon the presence of a

- significant market power (SMP) which is
- not-contestable, i.e. there is no prospect of any other market participant actually or potentially challenging the dominant market player.

Competition or threat of potential competition may discipline any market dominant player, making the abuse of an existing market dominance highly unlikely. In such a case, there is no need for intervention by competition authorities or legislators.

Whether or not a hyperscaler actually enjoys a significant market power demands a thorough investigation requiring a proper delineation ("definition") of the market and an analysis of the market position of the market participant under investigation.

At the same time, any market analysis should include a test of the contestability of the market. Contestability is not given when serious barriers to market-entry exist.[351] Barriers to entry may be manifold. Often, they take the form of

- high sunk and fixed costs: Typically, new market players are faced with high costs for machinery, distribution, specialised personnel, etc. Some of these costs are sunk, i.e. they are not retrievable in case of a market exit.[352] Companies already active in the market do not have to

351 Stigler, G.J., (1968)
352 Panzar, J.C., Willig, R.D. (1977).

carry the same costs anymore. In extreme cases, this may lead to natural monopolies.[353] Given a natural monopoly, the duplication of the facility by the potential competitors is not economically viable or desirable. The reason for this may be that it is more cost efficient for one company to produce a good or service than for two or more undertakings to do so.

- technological barriers: In some cases, patents, licences or intellectual property rights hinder competitors to have access to the same technology as the monopolist has.

- Contractual barriers: Lock-in effects (e.g. because of high switching costs) may complicate the activity both of new entrants and of existing competitors of the dominant undertaking(s). It remains to be analysed whether competition for new – not yet locked-in – customers can sufficiently discipline the dominant undertaking(s).

We cannot give a conclusive answer to the question whether the hyperscaler market is currently exposed to players with a non-contestable market power as this demands a thorough market investigation by competition authorities. Nevertheless, the market shares (see page 12) hint that there may be reason for such investigation. At the same time, current market dynamics do not suggest problems, however this may well change in the future.

2.1.1.2.2 Step 2: Competition law vs sector-specific regulation

Following the finding of non-contestable significant market power on the hyperscaler market, two possibilities remain. Upon abusive behaviour of the dominant firm, classical competition law will apply and may halt the specific abusive behaviour. This may concern issues such as monopolistic prices, limited access rights to cloud infrastructure, high switching costs or low technical interoperability between providers.

Alternatively, policy makers may go further and introduce sector-specific regulation aimed specifically at market participants with a significant market power in a pre-defined market. All market participants found to have significant market power may be subject to pre-defined remedies of the sector-specific regulation, irrespective of the question whether they actually abuse their market power. In practice, this may take the form of a direct regulation of switching-costs, of interoperability requirements or of end-user-prices directed at cloud providers with a significant market power.

Clearly, such sector-specific regulation represents a significant intervention in entrepreneurial freedom and hence demands a convincing justification. Whereas sector-specific regulation has its merits and may well be justified in certain cases (see box below), we do not see convincing arguments for a sector-specific regulation of switching costs, interoperability requirements or the like for hyperscalers.

First, the existing sector-specific regulation – especially in the telecom markets – aims at preventing competition problems associated with vertically integrated firms having a significant market power on the market for an essential physical facility (e.g. the telecommunication network). The privileged position of those – often privatised – incumbents endangers meaningful competition on the aftermarkets for services delivered on those facilities. Sector-specific regulation aiming at hyperscalers' switching costs or setting out interoperability requirements do not exhibit this vertical character, but focus on potential problems on the primary market of cloud services only. Given this fundamental

[353] Knieps, G. (2008), p. 25.

difference, regulating a dominant cloud service provider, based on the presence – not the abuse – of a dominant position only, seems disproportionate.

Second, sector-specific regulation is especially useful when market structures are clear, established and unlikely to significantly change in the near future. This has long been the case in the telecommunication market where the incumbent has been in possession of a large physical network and most competitors were reliant upon the use of that infrastructure in order to deliver their services. A comparable situation is not given in the hyperscale cloud service market. Although the number of hyper infrastructure providers is indeed limited, these competitors are in a similar situation and given fierce competition, the outcome of the competition process is not clear yet.

Third, markets in the existing sector-specific regulation for telecom markets are national. As a consequence, (sub)national markets have been defined and analysed to identify any significant market power on those markets. This process demands significant resources, which are spread over national authorities. If these cases were treated via general competition law, the EU-Commission's resources might not be sufficient. This is markedly different when looking at the hyperscale cloud market. Any market actor found to have a significant market power is likely to possess that power within the entire EU, neutralising some of the comparative practical advantages of sector-specific regulation.

The merits and risks of sector-specific regulation

In the EU, ex-ante sector-specific regulation is typically enforced by specialised national regulatory authorities and not by competition authorities.[354] The most developed ex-ante sector-specific regulation system in the EU is arguably the regulation of the telecommunication sector. A detailed set of European Directives[355] sets outs the preconditions, procedures and regulatory remedies which national regulatory authorities must apply. The EU-Commission possesses certain veto-powers against national action. This framework enables **swift** action.

This ex-ante approach has the advantage of being comparatively **clear and predictable and it reduces uncertainty** for both the dominant market player and its competitors. On the other hand, competition law always entails an assessment of the peculiarities of a single case. In that sense, the application of competition law is usually more precise and exact. However, having to assess each and every case takes time, which risks large delays in the imposition of supervisory measures, at the detriment of competition.[356]

Ex-ante regulation comes in before problems arise but is dependent upon relevant markets being pre-defined. It makes implicit assumptions on future market developments and the respective reactions of all (potential) market players. The ex-post concept of competition law, on the other hand, takes factual market information and data into account to judge whether a dominant undertaking exploits its market power. Hence, ex-ante regulation bears an **inherent risk of faulty and unnecessary regulation**.

354 In Germany, for instance, the Federal Network Agency (Bundesnetzagentur) is responsible for implementing regulatory measures a.o. in the field of telecommunication.

355 Framework Directive (2002/21/EG), Access Directive (2002/19/EG), Authorisation Directive (2002/20/EG), Universal Service Directive (2002/22/EG) and Data Protection Directive (2002/58/EG).

356 Van Roosebeke (2008), p. 14.

The framework for ex-ante regulation makes it fast, but also less flexible in its application. This brings about the risk of regulation being more persistent than ex-post control.[357] There is hence a **risk of over-regulation.**

Whatever way the authorities choose, there are two mistakes they may make. They may choose to regulate, although there is no need to do so. In this case, regulation would distort competition that actually functions (Type I Error). Or they may choose not to regulate, although there is a need to do so, because non-contestable market power is present. In this case, competition forces are too weak, prices too high and total output too low (Type II Error).[358]

Box 2: Merits and risks of sector-specific regulation.

2.1.1.3 Recommendation No. 10

Recommendation No. 10

The market for large scale cloud services (hyperscaler market) is currently characterised by intense competition amongst a relatively small number of competitors facing high fixed costs. It remains to be seen whether the current level of competition will prevail also in the future.

In any case, public intervention – e.g. by regulating switching-costs between cloud providers, interoperability requirements or end-user-prices – which is motivated by competition concerns should take place only given proof of a significant and non-contestable market power (SMP) of a cloud service provider.

Upon proof of such market power, competition law seems well able to offer an appropriate answer. The use of sector-specific regulation addressing dominant cloud service providers is not recommended.

2.1.2 Problem case 2: Abusive behaviour on the PaaS-Market

2.1.2.1 Description of the problem

On the market for platforms as a service (PaaS), platforms are provided to users in order to develop, manage and deliver applications. Similar to the IaaS-market, concentration on the PaaS-market is relatively high, with the three main players accounting for roughly 60% of the market in 2018 (see page 12).

Concentrating on PaaS-providers which are not vertically integrated[359] (i.e. not offering software on the SaaS-market in a notable scope), competition problems may arise if only a limited number of platforms are available.

Whether a PaaS-provider can achieve significant market power has to be investigated on a case-by-case basis. Indirect network effects make dominance problems more likely, as PaaS are two-sided platforms becoming more interesting to users when more application providers offer their services on the platform (and vice versa). Also, platform providers may use output-data as an input-factor to increase the quality of their product (see page 64). High fixed-costs and vendor lock-in problems also increase the likelihood of market power. On the other hand, product differentiation between B2B-

357 Ibid., p. 3 and 4.
358 Ibid., p. 12.
359 Vertical integration issues are dealt with below.

platforms, high levels of innovation and multi-homing by corporate users may lower the probability of market dominance (see page 14).

2.1.2.2 The appropriate policy

Any policy in reaction to competition issues on the non-vertically integrated PaaS-market must start from the finding of a non-contestable market dominance. The appropriate policy to these PaaS-issues should follow the same principles as those laid out for the IaaS-market.

The same arguments speaking against a sector-specific regulation – e.g. regarding admissible prices for software suppliers for accessing the platform – apply here as well. Moreover, for PaaS, intellectual property rights of the PaaS-provider may play a significant role. Even when in possession of a dominant market position, the platform provider's innovation efforts deserve protection (for more details, see below). It may be challenging – although not impossible – to incorporate such elements into sector-specific regulation.

2.1.2.3 Recommendation No. 11

Recommendation No. 11

Whether a PaaS-provider holds significant market power has to investigated on a case-by-case basis. In any case, the finding of a non-contestable market dominance of a platform provider should be a pre-condition for competition-based intervention. If proven, such dominance can be dealt with appropriately using general competition law. A need for sector-specific regulation is not evident.

2.1.3 Problem case 3: Vertical integration and privileged infrastructure access on the PaaS-market

2.1.3.1 Description of the problem

2.1.3.1.1 Tying and Bundling

As providers of large-scale cloud services integrate vertically by offering services on the PaaS-market, they may attempt to increase their chances of success on the PaaS-market by tying/bundling practices. In this scenario, cloud providers might make the use of their cloud services conditional upon the client also using the provider's platform on the PaaS-market. Alternatively, users may be offered preferential contractual conditions and prices when using both cloud and platform services of a provider.

2.1.3.1.2 Cloud infrastructure as an essential facility

Also, absent tying/bundling, the vertical integration of IaaS-providers into the PaaS-market may have consequences for the competition on the PaaS-market. Vertically integrated IaaS-providers may refuse other suppliers of PaaS-services (or users of those platforms) the use of their cloud-services. This may obstruct PaaS-suppliers in offering their services, as access to large scale cloud infrastructure may be a necessary condition ("essential facility") for offering platform services. Without such access, competition on the PaaS-market may deteriorate.

2.1.3.2 The appropriate policy

2.1.3.2.1 Tying and Bundling

From a competition point of view, tying and bundling practices are problematic only when used as a means to transfer a market power from an upstream market to downstream market. In such a sce-

nario, the tying/bundling constitutes an abuse of dominance. Hence, any competition-based policy measure targeting tying/bundling practices between the IaaS and Paas-market is convincing only once a non-contestable significant market power on the IaaS-market by the provider under investigation has been found (see 2.1.1). Without proof of such market power, tying/bundling practices between the IaaS and PaaS-markets are unproblematic from a competition-law point of view, although they may well have consequences for the level of competition on the PaaS-market (see 2.1.2 for other factors influencing the level of competition).

2.1.3.2.2 Cloud infrastructure and the essential facilities doctrine

Absent tying or bundling, vertically integrated cloud service providers which limit the access by competitors on the PaaS-market to cloud infrastructure may cause serious competition problems which demand intervention. Such intervention by competition authorities may mirror the essential facilities doctrine.

The essential facilities doctrine in competition law

Over the years, the Commission, the Court of Justice (ECJ) and the General Court (EGC) have developed the "essential facilities doctrine" which is a subset of abuse of a dominant position. Under certain conditions, denial of access to an "essential facility" may constitute an abusive exclusionary conduct according to Article 102 (2) (b) TFEU.[360] An essential facility can be a product, a service, an infrastructure like a harbour[361,362,363], a distribution system like a telecommunications network or an intellectual property like works protected by copyright or inventions protected by patents.[364]

When the essential facility is an intellectual property, a balance is struck between intellectual property law – aiming at fostering innovation by granting exclusive rights to rightsholders, which protects their incentives to invest time and effort in risky innovations – and undistorted competition – which creates innovation pressure and encourages efficiency.[365]

The ECJ and EGC have made clear that the denial of access to intellectual property by a rightsholder can be an abusive behaviour according to Article 102 TFEU under **exceptional circumstances**.[366] The Courts have subsequently (in: Magill[367], Bronner[368], IMS Health[369] and Microsoft[370]) set out that the exceptional circumstances are given, when:

(1) The use of an upstream facility is **indispensable** to carrying on the downstream business, i.e. there must be no actual or potential substitute for the facility the competitor seeks access to.[371] An

360 Koenig, C. and Schreiber, K. (2010). However, the essential facilities doctrine is classified by some as a category of Article 102 (1) TFEU, for example by Immenga/Mestmäcker (2012), Art. 82 EGV, paragraph 239.
361 Commission decision 11 June 1992, COMP/34174 – Sealink/B&I – Holyhead.
362 Commission decision 21 December 1993, Official Journal 1994, No L 15/8 – Sea Containers/Stena Sealink.
363 Commission decision 21 December 1993, Official Journal 1994 No 55/52 Port of Rødby.
364 Mestmäcker/Schweitzer (2014), § 19 paragraph 75.
365 Körber (2004), p. 881.
366 ECJ, Judgment in Magill, C-241/91 P and C-242/91 P, ECLI:EU:C:1995:98, paragraph 50.
367 ECJ, Judgment in Magill, C-241/91 P and C-242/91 P, ECLI:EU:C:1995:98.
368 ECJ, Judgment in Bronner, C-7/97, ECLI:EU:C:1998:569.
369 ECJ, Judgment in IMS Health, C-418/01, ECLI:EU:C:2004:257.
370 EGC, Judgment in Microsoft, T-201/04, ECLI:EU:T:2007:289.
371 ECJ, Judgment in Bronner, C-7/97, ECLI:EU:C:1998:569, paragraph 41; ECJ, Judgment in Magill, C-241/91 P and C-242/91 P, ECLI:EU:C:1995:98, paragraph 52 f.

actual substitute needs not be as "advantageous" as the facility itself.[372] A potential substitute is not given when there are technical, legal or even economic obstacles which make it impossible or unreasonably difficult for any other undertaking to establish its own facility.[373]

Economic obstacles are not given for a small competitor arguing that the creation of a new facility is "not economically viable"[374] to him, due to his size. Decisive is, whether the creation of a new facility is economically viable for a competitor that is "comparable" to the undertaking running the existing facility.[375] Moreover, possible losses in the short term do not make an investment "not economically viable".[376] However, the EGC ruled in *Microsoft* that access must be granted "on an equal footing".[377] This has been considered as a lowering of the indispensability criteria.[378] Since Microsoft did not appeal the EGC's judgment, the ECJ was not able to clarify its position on the EGC's modification of the indispensability criteria in its *Microsoft* judgment.

(2) The denial of access to the facility must be **likely to eliminate effective competition in the downstream market**.[379] In its *Microsoft* judgment, the EGC stated that there is no need to wait until there is (practically) no more competition on a market, because the objective of Article 102 TFEU is to maintain "undistorted competition".[380] According to the EGC, this is all the more true, if the market concerned is characterised by significant network effects which make it difficult to reverse an elimination of competition.[381] The Commission has pointed out that it would investigate whether the denial of access would lead to innovative goods or services not being brought to market and/or whether follow-on innovation is likely to be stifled.[382]

(3) The denial of access to a facility which is an **intellectual property** must prevent the appearance of a **new product or must limit technical development**.[383,384] The new product criterion is not a general criterion of the essential facilities doctrine, but applies in cases where a (potential) competitor seeks access to a facility which is an intellectual property.[385] An access-seeker intending to essentially duplicate the existing product or service on the downstream market by the owner of a facility which is an intellectual property, must not be offered access. Access must be granted only given the intention to produce a new product for which there is a potential consumer demand.[386] However, in *Microsoft* the EGC ruled that it may be sufficient to investigate whether denial of access limits technical devel-

372 ECJ, Judgment in Bronner, C-7/97, ECLI:EU:C:1998:569, paragraph 43.
373 ECJ, Judgment in Bronner, C-7/97, ECLI:EU:C:1998:569, paragraph 44.
374 ECJ, Judgment in Bronner, C-7/97, ECLI:EU:C:1998:569, paragraph 45.
375 ECJ, Judgment in Bronner, C-7/97, ECLI:EU:C:1998:569, paragraph 46.
376 Opinion of Advocate General Jacobs delivered on 28 May 1998 in Bronner, C-7/97, ECLI:EU:C:1998:569, paragraph 68.
377 EGC, Judgment in Microsoft, T-201/04, ECLI:EU:T:2007:289, paragraph 421.
378 Graef, Wahyuningtyas, Valcke (2015), Körber (2007)
379 ECJ, Judgment in Magill, C-241/91 P and C-242/91 P, ECLI:EU:C:1995:98, paragraph 56.
380 EGC, Judgment in Microsoft, T-201/04, ECLI:EU:T:2007:289, paragraph 561.
381 EGC, Judgment in Microsoft, T-201/04, ECLI:EU:T:2007:289, paragraph 562.
382 Communication from the Commission — Guidance on the Commission's enforcement priorities in applying Article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings, Paragraph 87
383 ECJ, Judgment in Magill, C-241/91 P and C-242/91 P, ECLI:EU:C:1995:98, paragraph 54.
384 EGC, Judgment in Microsoft, T-201/04, ECLI:EU:T:2007:289, paragraph 647.
385 Böttcher (2011), p. 25.
386 ECJ, Judgment in IMS Health, C-418/01, ECLI: EU: C:2004:257, paragraph 49.

opment[387]. This ruling is interpreted by some as a lowering of the new product criterion,[388] by others as a questioning of the new product criterion.[389]

(4) The denial of access to an essential facility may be justified by **objective reasons**.[390] In its *Microsoft* judgment, for instance, the EGC discussed the question whether granting access could have a negative impact on Microsoft's incentives to innovate.[391]

Box 3: The essential facilities doctrine in competition law

The essential facilities doctrine can be applied to vertically integrated cloud providers which refuse access to their cloud infrastructure for competing PaaS-providers only given the following conditions:

(1) There is no actual or potential substitute to the cloud infrastructure to which access has been refused. In essence, this means that the cloud provider must hold a non-contestable market dominance on the relevant cloud infrastructure market (see 2.1.1).
(2) Denial of access to the dominant cloud providers' infrastructure must be likely to eliminate effective competition on the PaaS-market. In other words, the use of cloud infrastructure must be necessary to successfully offer PaaS-services and network effects may make it very difficult to contest an existing vertically integrated and dominant enterprise.
(3) As the cloud providers intellectual property rights deserve protection, any access-seeker on the PaaS-market must offer a certain novelty, beyond what the cloud infrstructure provider already offers on the PaaS-market. Given limited case law, it is not fully clear whether PaaS-providers must offer new products or whether it is sufficient that the refusal of access may limit technical development.[392]
(4) The cloud provider does not bring forward convincing objective reasons, e.g. concerning the cloud provider's incentives for innovation.

If these conditions were met, the essential facilities doctrine allows competition authorities to force a vertically integrated cloud provider to grant a PaaS-provider regulated access to its infrastructure.

2.1.3.2.3 Sector-specific regulation

The merits of sector-specific regulation fit rather well to the characteristics of the case where a vertically integrated cloud provider refuses PaaS-providers access to its infrastructure. Assuming that the use of cloud infrastructure is essential for offering PaaS-services, in order to respect the principles of competition law, it is essential that the scope of any such regulation is limited to dominant cloud providers. Any sector-specific regulation would have to entail a mechanism for defining and analysing cloud markets as well as for investigating the market power of providers on those markets.

However, the most challenging part of any sector-specific regulation regards the protection of intellectual property rights. Merely holding a dominant market position on an essential facility market should not "automatically" lead to a regulated access obligation. Authorities will have to make a case-by-case decision whether intellectual property rights that deserve protection are present; and if yes, how this protection can be guaranteed. It is difficult to standardise the answer to this question in

387 EGC, Judgment in Microsoft, T-201/04, ECLI:EU:T:2007:289, paragraph 647.
388 Graef, Wahyuningtyas, Valcke (2015), p. 382
389 Körber (2007)
390 ECJ, Judgment in Magill, C-241/91 P and C-242/91 P, ECLI:EU:C:1995:98, paragraph 55.
391 EGC, Judgment in Microsoft, T-201/04, ECLI:EU:T:2007:289, paragraph 696 et seq.
392 EGC, Judgment in Microsoft, T-201/04, ECLI:EU:T:2007:289, paragraph 647.

a set of possible remedies laid down in sector-specific regulation. Authorities may find it appropriate to not impose access obligations, or they may impose access but do so at regulated costs which reflect the intellectual protection they deem appropriate.

All this does not make sector-specific regulation unfit to deal with these competition challenges. However, it reduces the comparative advantages of such regulation, such as swiftness and the advantage of being clear, predictable and reducing uncertainty. In addition, given that cloud markets can be expected to be transnational instead of national, the number of dominant cloud providers in the EU – if any – can be expected to be very small. Hence, if a very small number of cases are up to decision anyway, competition law may do the job just as well.

2.1.3.3 Recommendation No. 12

Recommendation No. 12

Tying and bundling practices by cloud providers which vertically integrate into the PaaS-market are unproblematic, unless those providers hold a non-contestable market power on the cloud infrastructure markets. If they do, competition law is well fit to cope with this abusive behaviour.

Absent tying and bundling, the refusal by a vertically integrated cloud provider to grant PaaS-competitors access to its cloud infrastructure can be dealt with using the essential facilities doctrine. This doctrine offers a convincing trade-off between the protection of intellectual property rights and safeguarding competition on aftermarkets. The need for intervention is limited to cases where the following criteria are fulfilled: (1) the cloud provider holds a non-contestable dominance on the cloud market, (2) the use of the cloud is imperative, (3) competing PaaS-providers offer a novelty and (4) the cloud provider cannot offer objective reasons justifying the refusal of access.

Although a sector-specific access regulation regime may be able to cope with dominant, vertically integrated cloud providers on the PaaS-market, clear advantages of such regulation as compared to general competition law are not apparent.

2.1.4 Problem case 4: Vertical integration and privileged data access on the SaaS and other markets

2.1.4.1 Description of the problem

2.1.4.1.1 Essential data and the SaaS-market

The full vertical integration of market participants active on the IaaS, PaaS and SaaS-markets may cause competition problems on the SaaS-market. Under certain circumstances, IaaS- and PaaS-providers may be technically and legally able to use users' data stored on their infrastructure or running via their platforms. This data may offer them a competitive advantage regarding the development of SaaS-products. Competing SaaS-providers, which are not vertically integrated to the same extent, may not have access to comparable data. Also, the network effects of the IaaS and PaaS-markets may make it very difficult for those SaaS-providers to build a comparable data pool through IaaS and PaaS-activities. In market segments where the added value of the data analysis to developing SaaS-products is substantial, this may impede competition on the SaaS-market.

2.1.4.1.2 Essential data on other markets

This problem must not necessarily be limited to market participants which are vertically integrated over the IaaS, PaaS and SaaS-markets. A privileged access to data may also arise because of an eco-

nomic activity in other upstream markets. As an example, the privileged access to data by vertically integrated manufacturers of industrial machinery may cause competition problems on maintenance aftermarkets.

2.1.4.2 The appropriate policy

Privileged data access is a competition problem if the data is an "essential facility" to the development of a downstream product. In the following, we treat some of the most crucial criteria for applying the essential facility doctrine to data related competition problems. We do so using two examples, i.e.: the SaaS-market and the machinery maintenance market.

2.1.4.2.1 Definition of the upstream data market

Any use of the essential facilities doctrine presupposes the definition of an upstream as well as a downstream market. The downstream market may be the SaaS-market or a maintenance market; the upstream market – on which the alleged essential facility is to be found – may be a market for data. Note that this market for data must not already exist, it may also be a hypothetical market.[393]

Obviously, depending on the downstream market under investigation, the definition of the upstream market may differ. Where data is seen as an upstream market, it is important to understand that data is not a homogeneous good.[394]

In the first example discussed here, the upstream data market relevant to **SaaS-products** may consist of business-related data which has been generated on Enterprise-Resource-Planning systems. This data may consist of personal and non-personal datasets as well as mixed datasets and may be stored on the infrastructure of a vertically integrated cloud service provider. Depending on the downstream SaaS-market under investigation, personal data sets which are produced in a B2C context – e.g. by using of search engines – may also be relevant. Hence, the relevant "data market" must not necessarily be directly connected to the IaaS-market.

Where the aftermarket is one for **maintenance of industrial machinery**, the upstream market may consist of machine generated data, produced by sensors in industrial equipment and forwarded on a continuous basis to the producer of the machinery.

Concluding, any useful application of the essential facilities doctrine will require competition authorities to differentiate between different data types and subsequent markets[395] on a case-by-case basis, as the kind of data relevant for a given downstream product may be very different.

2.1.4.2.2 Market dominance and data as essential facility

For the essential facilities doctrine to be relevant, there must be an undertaking with a dominant market position in the defined upstream data market. The fact that data is ubiquitous and non-rival is not sufficient to per se exclude a dominant position.[396] Obviously, the exact delineation of the upstream data market will be essential in finding dominance (or not). This will in turn depend upon how narrow the downstream product/service market has been defined. When considering only a subset

393 ECJ, Judgment in IMS Health, C-418/01, ECLI: EU: C:2004:257, paragraph 49
394 See page 15
395 Graef (2016), p. 258
396 Id., p. 260; Kathuria, V. and Globocnik, J. (2019)

of SaaS-products or maintenance of a (brand) specific industrial machinery, the likelihood of finding a dominant position will rise.[397]

Companies with a dominant position in the relevant upstream data market are not required to deal on these markets – simply because they hold a dominant position – with companies with whom they compete on the downstream market.[398] For this to be required, the use of the data must essential, i.e. "objectively necessary to compete effectively on the market".[399]

Whether and when the defined data is an "objectively necessary" (essential) input for the SaaS-market or the industrial maintenance market, obviously must be decided on a case-by-case basis. The Commission's guidance allows to conclude that even without use of the "essential data", a competitor may be able to enter or survive on the downstream market. What is relevant, is whether an actual or potential data-substitute is available to downstream competitors that counters — at least in the long-term — the negative consequences of the lacking access to the essential data.[400]

In other words, the question is whether the relevant upstream data (in the possession of market dominant enterprise) is duplicable. In the data context, legal and economic problems may make this difficult. Regarding economic problems however, the "as-efficient competitor test" applies, i.e. the relevant question is, whether a second data provider of similar size and efficiency can survive in the market.[401]

When investigating whether data can be an essential input on **SaaS-markets**, the following has to be considered:

- Big data and AI-techniques may be advantageous in developing SaaS-products and the availability of data from different corporate sources may improve the actual added-value of using those services.
- This data – in its specific shape and form – is typically stored on the infrastructure of a very limited number of hyper cloud providers. It is important to consider here:
  - Do cloud providers have access to users' data at all? Currently, this practice does not seem to be widespread, at least with regard to business data. A potential decrease in the level of competition may change that. Without such access on the side of cloud providers, market dominant actors on upstream data market are non-existent.
  - Even upon having access to users' data, the co-existence of a (admittingly small) number of other cloud providers may have a discipling effect and prevent market dominance.
  - Data stored on hyper cloud providers' infrastructure is not fully comparable to a classical essential facility in the hands of an upstream enterprise. In fact, although cloud providers *might* be able to use (i.e. analyse) the data, the cloud customer may be in a position to allocate its data elsewhere. Depending on the level of competition on the IaaS-market, the customer may move its data to another cloud provider (in which case market dominance on the upstream data market is unlikely) or may even make

397 See Whish and Bailey (2018), p. 36 with examples of narrowly defined aftermarkets for spare parts.
398 Whish R. and Bailey D. (2018)
399 EU-Commission (2009), Paragraph 83
400 Id.
401 Mestmäcker and Schweitzer (2014), § 19. Behinderungsmissbrauch Rn. 66 - 80, beck-online

its data directly available to the SaaS-provider. Whether or not this is feasible depends upon a number of legal and economic questions. Legal matters may concern lock-in effects on the side of cloud customer where contractual clauses or technical incompatibilities may cause high switching costs. Economic questions may concern the question whether a hyper cloud can be seen as a natural monopoly. Upon examining this, economics of scale and scope but also network effects should be taken into consideration.[402]

- Can on-premise data be seen as a substitute to cloud data? If not, can it be seen as a potential substitute, disciplining cloud providers?

Looking at whether **machine generated data** can be an essential facility for the maintenance aftermarket, the following has to be considered:

- Is a market dominance given on the upstream data market? The exact definition of the downstream market will have a considerable impact on this question and hence on the applicability of the essential facility doctrine. A brand-specific market definition is more likely to lead to the finding of a market dominance on the related data market, and if so, this will most likely be the machine manufacturer.
- Whether or not machine-generated data is duplicable is likely to depend on technical and contractual issues. Both barriers may cause a lock-in and may prevent the physical transfer of data to any other player than the dominant one. Such barriers can be machine-typical or be part of the contractual relation between the seller and buyer on the primary market. They are more likely to occur on primary machinery markets with a dominant supplier.

2.1.4.2.3 Problems related to granting access to essential data

The finding of an essential data facility may lead to the conclusion that a competition-law based obligation for the company enjoying dominance on the relevant data market to grant access to this data is appropriate. However, putting such an obligation into practice may proof challenging for a number of reasons.

- First, the data access obligation may refer to both personal or non-personal data of third parties. This raises a number of **data protection** issues.

  It must be cleared under which circumstances an obligation to grant access to personal data is in accordance with the GDPR. Although the GDPR allows for processing of personal data - also without explicit consent, when this "is necessary for compliance with a legal obligation to which the controller is subject"[403], a mere – essential facilities based – obligation under European competition law is not a sufficient condition for the sharing of such data.[404] In any case, an additional legal basis for this sharing must be established, preferably in EU-law.[405] Such legal basis shall contain the purpose of the data processing as well as specific provisions regard-

402 Graef (2016), p. 261
403 Art. 6 para. 1 lit. c GDPR
404 Demary V., Guggenberger N., Rabovskaja E. and Rusche C. (2019) and Crémer J., de Montjoye Y., Schweizer H. (2019)
405 Art. 6 para. 3 GDPR

ing the general condition of lawful processing as well as the types of data concerned or the entities to which data may be disclosed.[406]

To safeguard the application of the essential facilities doctrine, we recommend the Commission to propose such legal basis. It is obvious that this in effect represents a conflict between competition law and data protection. The specific provisions of the legal basis may reflect this, e.g. by mandating an examination whether the purpose of data processing can be reached also by means of anonymised personal data. However, such a legal basis can only legitimise the transferring of the data, not the processing of the data by the access seeker. For this purpose, an additional consent by the data subject seems necessary.[407]

Similar problems may arise when data access rights affect non-personal data. Data subjects may oppose a data transfer, claiming business and trade secrets. If technical and contractual clauses allow so, those data subjects can be expected to withdraw their data from the disposal of the data holder and this may make the data access factually meaningless.

- **Pricing** issues may also proof an obstacle to data access obligations. Any data access will not be priceless. Competition authorities will be tasked to set a price to accessing data, those prices will have to include a proportionate protection of the intellectual property rights of the data holder. Given the perishable nature of data, such pricing may be a challenging task.

- Also, it may be difficult to exclude that data is being sold on or also being used for **other purposes** very different to those aimed at by competition authorities. This does not only make pricing of data very difficult but more importantly, it may have very adverse effects on other markets and on the incentive for innovation on those markets.

All in all, the practical possibilities of data access obligations under the competition law's essential facilities doctrine may be rather limited.

2.1.4.2.4 Alternative remedies to data access

When – upon finding a dominant market position on a well-defined upstream data market – imposing data access turns out to be impractical, competition authorities should turn to other remedies that render the data "non-essential".

- In the area on vertically integrated IaaS-providers, remedies or regulatory measures that ease the switching of cloud providers by users and lower technical barriers to doing so, may contribute to avoiding a lock-in position on the IaaS-market. Depending on the characteristics of the SaaS-market, stronger portability rights, if necessary in real-time via APIs might be installed.
- In other areas, it may be necessary to safeguard the possibility of data subjects to transfer data to another downstream service provider, irrespective of the terms of contract of the dominant market participant.[408]

Importantly:

406 Id.
407 Demary V., Guggenberger N., Rabovskaja E. and Rusche C. (2019), p. 78
408 Similar: Bundesministerium für Wirtschaft und Energie (2019a), p. 41

- Both remedies should apply only to market players which are dominant on the well-defined upstream data market. A general obligation to all market players would deter competition and unnecessarily limit contractual freedom.
- Any remedy must duly protect the intellectual property rights of the market dominant firm, e.g. by allowing it to differentiate prices, depending on whether the data transfer right is actually activated.

There is no general answer to the question whether these remedies are to be implemented by competition authorities or through general regulation. It is however of utmost importance that they apply only to market participants with a dominant position in well-defined markets. In cases where markets are defined very narrowly (e.g. brand-wise), the finding of market dominance may be rather straight-forward and regulation may be appropriate. In all other cases, competition law can better guarantee an appropriate market definition and analysis of market dominance.

2.1.4.3 Recommendation No. 13

Recommendation No. 13

Privileged data access may hinder competition. This goes for all product and service markets, in which data is an essential input. On the SaaS-market, the vertical integration of IaaS-providers down to the PaaS and SaaS-markets and the associated market concentration may aggravate the competition problems on the SaaS-market associated with privileged data access. Also, privileged access to data may cause competition problems in very different downstream markets.

With the essential facilities doctrine, competition law offers a sound fundament to deal with competition issues in respect with vertical integration. However, in practice, if data turns out to be the essential facility, access-granting may prove to be very difficult and unpractical. In that case, alternative remedies or regulatory interventions that prevent data being or becoming an "essential facility" may be necessary. Such interventions should aim at increasing data portability, be it by lowering barriers to switching and preventing lock-in situations or by granting direct portability rights.

However, when doing so, intellectual property rights must be given due consideration. In any case, the finding of a dominant market position in the absence of potential competition on a well-defined upstream data market must be a precondition for any intervention. In cases where markets are defined very narrowly (e.g. brand-wise), the finding of market dominance may be rather straight-forward and regulation may be appropriate. In all other cases, competition law can better guarantee an appropriate market definition and analysis of market dominance.

2.2 Anti-competitive agreements and data pooling

A data pool is a kind of data sharing system "*which involves an element of reciprocity, whereby at least some companies contribute data*".[409]

Data pooling arrangements are generally pro-competitive in so far as "[t]*hey enhance data access, may resolve data bottlenecks and contribute to a fuller realisation of the innovative potential inherent in data. The pooling of data of the same type or of complementary data resources may enable*

409 European Commission, *Antitrust: Commission opens investigation into Insurance Ireland data pooling system*, Press Release, Brussels, 14 May 2019, accessible at https://europa.eu/rapid/press-release_IP-19-2509_en.htm

firms to develop new or better products or services or to train algorithms on a broader, more meaningful basis".[410]

However, data pooling arrangements expose the parties to antitrust liability. Depending on the circumstances of the case, a data pooling agreement could qualify as a forbidden information sharing agreement, allowing participants to collude, or as an abuse of collective dominance, consisting in a denial of access to competitors that are part of the network or in granting access to such competitors on non-FRAND terms. Also, due to the necessity of having data conferred to the pool in a specific format to allow mutual use, a data pooling arrangement could encompass a forbidden standard setting clause, which confines third parties out of the technology market.[411]

The antitrust review of the concrete terms of such horizontal cooperation can lead to dramatically different results depending on the technology chosen by the participants, the legal vehicles and the scenario framing it.

This makes it hard for companies to design "safe" data sharing agreements, especially because of the novelty of the issues involved, i.e. the substantial lack of guidance by the enforcement practice of the Commission or by the case-law of the CJEU. Recent studies have highlighted that the current state of legal uncertainty is negatively affecting data pooling, thus hampering innovation and efficiency gains within the internal market.[412]

As it will be illustrated in the following, this problem could be dealt with either by establishing safe harbours (see 2.2.1) or by introducing legal tools aimed at removing legal uncertainty on a case by case basis (see 2.2.2).

2.2.1 Data pooling agreements under a competition law perspective: safe harbours

"Safe harbour" is an expression referring to any rule that makes it harder to establish liability for certain business practices.[413]

Safe harbours mainly consist of legal presumptions, i.e. legal rules that infer an unknown fact from a known fact, thus creating the conditions for applying a certain legal regime without a full factual review. By eliminating the necessity of a previous, in-depth review, presumptions simplify the legal analysis and bring, as a consequence, additional legal certainty.

In the area of antitrust enforcement, safe harbours are not exclusively established to the benefit of undertakings. "*Courts and authorities have limited resources, so they cannot afford to seek absolute truth: they only seek to solve legal disputes with their limited resources. For this reason, courts and authorities look at the likelihood of events, not "certainty". When fact B is reasonably likely or certain, the benefit of ascertaining whether it is, in fact, true, is not necessarily worth the cost – not just the costs to the court, the competition authority, and the firms involved, but, mostly, the cost to the pub-*

410 Crémer J., de Montjoye Y., Schweizer H. (2019), p. 92

411 For a review of the competition concerns raised by data pools, see Crémer J., de Montjoye Y., Schweizer H. (2019), pp. 96 ff.

412 A New Competition Framework for the Digital Economy, Report by the Commission 'Competition Law 4.0', 9.09.2019, p. 62-63

413 OECD (2017a), p. 20

lic in terms of competition cases that are not pursued because resources are tied down on other cases".[414]

In this sense, safe harbours and more broad presumptions do not run counter a "more economic approach"; rather, they are the result of the incorporation within the more economic approach of the so called "decision theory", i.e. "*the economics of making optimal decisions in conditions where information is costly and resources are limited*".[415]

In the following, two kinds of presumptive regimes will be assessed as to their ability to effectively tackle legal uncertainty in the antitrust review of data pools agreements: block exemptions and guidelines.

2.2.1.1 Block exemptions

Article 101 TFEU prohibits agreements, decisions by associations of undertakings and concerted practices that may have as their object or effect the restriction of competition.

Its application relies on a two-step legal test: whereas Article 101(1) TFEU sets forth the above prohibition, and Article 101(3) TFEU provides for its inapplicability under specific circumstances. This is the case where an agreement or concerted practice contributes to improving the production or distribution of goods or to promoting technical or economic progress, while allowing consumers a fair share of the resulting benefit, and the agreement or concerted practice does not (a) impose on the undertakings concerned restrictions which are not indispensable to the attainment of those objectives, and (b) afford those undertakings the possibility of eliminating competition in respect of a substantial part of the products in question.

Block Exemption Regulations are secondary law instruments[416] that provide legal certainty by establishing the presumption that a certain category of agreements falling within Article 101(1) of the Treaty are to be regarded as satisfying all the conditions laid down in Article 101(3) of the Treaty, thus "*allowing some types of agreements to benefit from a sort of "safe harbour"*".[417]

2.2.1.2 Guidelines

Guidelines provide interpretative guidance by signalling scepticism, openness or strong reliance as to whether a particular circumstance calls for the application of a specific legal regime.[418] In this sense, like block exemptions, they embody a presumption, but, contrary to the block exemptions, they provide for a *weak* presumption.

Besides the very design of the legal rule (clear-cut exclusion of anti-competitiveness versus mere interpretative guidance), the relative weakness of the presumptions embodied in guidelines in respect to the presumption set forth within block exemptions depends upon the fact that guidelines

414 Ritter C. (2018), p. 17

415 Laitenberger J. (2018), p. 8

416 Formally, block exemptions should be laid down, as any other act of primary law giving effect to the principles set out in Article 101 TFEU, by the Council, on a proposal from the Commission and after consulting the European Parliament (Article 101 para. 1 TFEU). According to Article 101 para. 1 (b) TFEU, the regulations or directives referred to in paragraph 1 shall be designed in particular "to lay down detailed rules for the application of Article 101(3), taking into account the need to ensure effective supervision on the one hand, and to simplify administration to the greatest possible extent on the other". However, most commonly, the Council merely empowers the Commission to adopt such acts, which are therefore secondary law instruments.

417 OECD (2019), p. 4

418 Ritter C. (2018)

are soft law instruments. As such and unlike Block Exemption Regulations, they only bind the Commission to make use of the criteria thereby established when applying EU law provisions.[419]

2.2.1.3 Assessment

The use of presumptions in competition law is meant to ensure the administrability of enforcement: by simplifying it, presumptions direct the efforts of the authorities towards more serious infringements. Likewise, presumptions invariably improve legal certainty, as they shed some light on how competition law provisions are supposed to be applied in the future.

While those considerations play a role in establishing any kind of safe harbour, they are *per se* unable to justify the introduction of a *strong* presumption (i.e. of a block exemption regime), which must be backed by additional justifications. Arguably, the design of the presumption should be dependent upon the rationale governing its establishment: the higher the quality of the justification for the establishment of a presumption, the more stringent the presumption could and should be.

Ideally, the establishment of a robust safe harbour should rely on an equally robust analysis of the market, suggesting that market conduct of this kind will not have anticompetitive effects in most cases. The existence of a reliable and documented economic theory supporting the establishment of a safe harbour is another example of high-quality consideration advocating for a block exemption.

Such additional justifications are seemingly absent in the case of data pools, which are, so far "*a relatively new and under-researched topic in competition law* [whose economics are] *also not very well understood*".[420]

Therefore, the establishment of a block exemption regime for data pools does not seem to be adequately supported.

On the contrary, guidelines from the Commission would be very much welcome: while they would not set forth "hard" presumption regimes, they could prove precious for undertakings striving to assess the approach of competition authorities in uncharted territory, as data pool agreements are at the time. Even more so since Ms. Vestager has already expressed some indications on the topic.[421]

The Commission seems to share this idea as it has recently announced its intention to launch a review of its guidelines on horizontal cooperation agreements "*to ensure that the guidance provided*

---

419 Judgement of 19 July 2016, *Kotnik and Others*, C-526/14, EU:C:2016:570, points 40, 41. On the lack of binding character of Commission's guidelines for national authorities, see judgement of 13 December 2012, *Expedia*, C-226/11, EU:C:2012:795, point 31.

420 Crémer J., De Montjoye Y., Schweizer H. (2019), p. 93

421 "[C]ompanies have to make sure that the data they pool doesn't give away too much about their business. Otherwise, it might become too easy for them to coordinate their actions, rather than competing to cut prices and improve their products. One way to do that is by sharing information anonymously. Companies could send their data to a platform and get back aggregate data with no indication of which company it comes from. That would still give companies information that would help build better cars or make existing ones run better - it just wouldn't undermine competition. Or companies might limit the type of information they share. So car companies might decide not to share information that would tell rivals too much about their technology. Online shops might share data without saying when products were bought, or for how much" (Vestager M.(2016)).

continues to give market operators the tools to assess their cooperation agreements".[422] The initiative is supported by authoritative scholars.[423]

2.2.2 Data pooling agreements under a competition law perspective: individual decisions of the Commission

Legal certainty could be equally promoted by the Commission through the issuance of individual acts aimed at assessing whether particular characteristics of a specific data pool arrangement raise competition law issues or by providing informal guidance on contentious legal questions.[424]

The relevant legal tools in this regard are the findings of inapplicability (Article 10, Regulation 1/2003/EC) and informal guidance. Also, a new procedural instrument has been recently proposed by the German Commission 'Competition Law 4.0'. They will all be exposed in the following pages.

2.2.2.1 Findings of inapplicability

According to Regulation 1/2003/EC, "[i]*n exceptional cases where the public interest of the Community so requires, it may* […] *be expedient for the Commission to adopt a decision of a declaratory nature finding that the prohibition in Article 81 or Article 82 of the Treaty does not apply, with a view to clarifying the law and ensuring its consistent application throughout the Community, in particular with regard to new types of agreements or practices that have not been settled in the existing case-law and administrative practice*" (recital n. 14).

Under Article 10 para. 1 Regulation 1/2003/EC, "[w]*here the Community public interest relating to the application of Articles 81 and 82 of the Treaty so requires*", the Commission may decide, *inter alia*, that Article 101 TFEU is not applicable to a specific agreement, decision by an association of undertakings or concerted practice, either because the conditions of Article 101(1) are not fulfilled, or because the conditions of Article 101(3) are satisfied. This decision also excludes the applicability of Article 101(2) and preserves, accordingly, the effectiveness of the covered agreements under a private law perspective.

According to the *Antitrust Manual of Procedures* issued by the Commission, "[t]*he Commission has exclusive competence and, within the limits set out in Article 10 of Regulation 1/2003* […] *as interpreted in the light of Recital 14, substantial discretion to take this type of decisions*".

The notion of 'Community public interest' is crucial to understand the objective of this provision. DG COMP expressed its views on the topic in its *Antitrust Manual of Procedures*, according to which the term 'Community public interest' must be understood as a reference to "*the fundamental commitment of the European Union to a system of undistorted competition as a common public goal*".[425] Accordingly, first, a declaratory decision of the kind envisaged by Article 10 Regulation 1/2003/EC can be proposed in exceptional cases where the consistent application of competition law throughout the EU is endangered. This is the case when a Commission decision is needed (i) to "correct" the ap-

---

422 European Commission, *Antitrust: Commission opens investigation into Insurance Ireland data pooling system*, Press Release, Brussels, 14 May 2019, accessible at https://europa.eu/rapid/press-release_IP-19-2509_en.htm

423 "There may be a need to revisit Chapter 2 of the 2011 Guidelines in light of the more recent case law, novel findings in economics and data science, and questions raised by the data economy" (Crémer J., De Montjoye Y., Schweizer H., p. 96).

424 *A New Competition Framework for the Digital Economy*, Report by the Commission 'Competition Law 4.0, 9.09.2019, p. 61.

425 EU-Commission (2012)

proach of a national competition authority on a specific issue; or (ii) to send a signal to the European Competition Network about how to approach a certain case.[426]

Secondly, in the view of the Commission, the use of the term "Community public interest" in Article 10 and the limitation of this legal tool to "exceptional cases" as of recital 14 are meant to exclude the adoption of such decisions to fulfil the interests – as legitimate as they may be – of individual companies, i.e. to avoid this instrument being used as a replacement for the exemption decision under the old system.[427] Only the necessity to safeguard the coherence of competition policy across the EU "*can justify allocating the Commission's resources to the preparation of this type of "positive" decision*".[428]

According to this approach, the novelty of the competition law issue raised by the agreement under consideration *per se* is irrelevant under Article 10 para. 1 Regulation 1/2003/EC. It only becomes relevant in so far as it is dealt with at the same time by national competition authorities and courts: in this case, due to the risk of divergent application of competition rules, a clarification by way of an Article 10 decision may be appropriate. "*However, recourse to an Article 10 decision in such a situation should normally only be had if other means of preventing the risk of divergence, such as an amicus curiae intervention of the Commission in proceedings before national courts, will likely not be sufficient*".[429]

The Commission's interpretation of Article 10 para. 1 Regulation 1/2003/EC is so strict that it has not until now adopted any decisions based on it and there is no indication that things will change in the future.[430] Besides, the findings of inapplicability are not intrinsically designed to address legal uncertainty issues and are therefore of little use here.

2.2.2.2 Notices of informal guidance

According to recital 38 of Regulation 1/2003/EC, "[w]*here cases give rise to genuine uncertainty because they present novel or unresolved questions for the application of these rules, individual undertakings may wish to seek informal guidance from the Commission*". The framework governing the substantial and formal conditions for requesting informal guidance as well as its effects is set forth by the Commission's Notice on guidance letters.[431]

According to the latter, a request for guidance can only be successful if the following cumulative conditions are met:

- the case presents novel or unresolved questions concerning the application of Articles 101 and 102 TFEU;

426 EU-Commission (2009c), p.36, para. 113

427 The system through which Article 101(3) TFEU was applied before Regulation 1/2003 was a centralised notification and authorisation system. The existence of the requirements for Article 101(3) TFEU to apply was therefore reviewed *ex ante* and on a case by case basis by the Commission. For an illustration of the different steps of the reform and the reasons supporting it, see Wils (2013).

428 EU-Commission (2012)

429 EU-Commission (2012)

430 While the interpretation illustrated above is without prejudice of the interpretation of the CJEU, the Commission has a lot of discretion in deciding if and how to use such power; all the more so since, under Article 10 para. 1 Regulation 1/2003/EC, such decisions cannot be requested and can only be taken at its own initiative. The Commission's approach to the conditions governing the exercise of this power is therefore crucial.

431 EU-Commission (2004)

- such questions are relevant, e.g. because they regard widely spread market behaviours;
- the application contains all relevant information.[432]

As to the negative conditions provided for by the Notice, questions are not admissible (i) when addressing issues that do not fit with the Commission's enforcement priorities[433] and (ii) when they are purely theoretical.[434]

According to the Notice, informal guidance does not bind the Commission nor national courts and authorities.[435]

So far, the Commission has upheld no informal guidance request, due to its very strict application of the conditions of admissibility. Notably, it has consistently excluded the novel or genuinely uncertain character of the questions referred to it.[436] However, due to the major changes triggered by Big Data to the traditional tools of antitrust analysis, there is no reason to exclude that genuinely novel questions might arise and pass the strict admissibility test of the Commission.

2.2.2.3 Voluntary notification system for data pool agreements

The Commission 'Competition Law 4.0' (the Commission 4.0), set up by the German Minister of Economic Affairs, proposed the establishment of a voluntary notification system to the EU Commission.

The main benefit of the system for prospective participants in data pool agreements lies in a preliminary review of the Commission as to whether a specific planned agreement infringes Article 101 TFEU. This would give companies legal certainty about the admissibility of novel forms of cooperation under antitrust law.[437]

According to this proposal, the admissibility of such applications would depend upon the economic relevance of the project and the novelty of the question. DG COMP would need to deliver a decision as to the compliance of the project with Article 101 TFEU within 90 working days.[438]

In the view of the rapidly changing market conditions, the Commission 4.0 acknowledges that antitrust issues could materialise after the conclusion of the procedure. Therefore, as it already is the case for decisions on commitments pursuant to Art. 9 para. 2 (a) of Regulation 1/2003, the EU Commission should be able to annul the decisions in case of changes of circumstances.[439]

The above proposal promotes data pools by shifting the responsibility for their compliance with antitrust law from the undertaking to the EU Commission. While this is likely to increase the number of market actors willing to enter such agreements, the solution is not totally convincing.

First, if it is true that the assessment as to the compliance of such agreements with antitrust law is so complex, one might wonder how the EU Commission could be able to deliver such an analysis in such a short timeframe (90 days).

---

432 EU-Commission (2004), para. 8
433 EU-Commission (2004), para. 7
434 EU-Commission (2004), para. 10
435 EU-Commission (2004), para. 24, 25
436 EU-Commission (2009b), para. 45
437 Bundesministerium für Wirtschaft und Energie (2019a), p. 62
438 Bundesministerium für Wirtschaft und Energie (2019a), p. 62-63
439 Bundesministerium für Wirtschaft und Energie (2019a), p. 63

Secondly, the real added value of this option for companies, i.e. that they are shielded from Article 101 TFEU enforcement, is hindered by the fact that, in case of a change of circumstances, the EU Commission can open an infringement procedure against the agreement it gave a green light to. It should be underlined that, in high technology markets such as the ones where the affected undertakings operate, this change may well materialise and will make the above shield nugatory.

Thirdly, the restrictive interpretation consistently adopted by the EU Commission as to the "novelty of the question" requirement when asked for informal guidance, which also constitutes an admissibility requirement for applications under this voluntary notification system, needs to be taken in consideration while evaluating the proposal at hand. In this respect, it should be noted that it was exactly the restrictive interpretation of the "novelty" requirement that prevented the use of informal guidance and that there is no reason to suppose that the Commission will take a different stance towards applications for data pools clearance.

2.2.2.4 Assessment

In the view of the above, it can be concluded that the most valuable instrument to tackle legal uncertainty among the individual decisions presented above is informal guidance. The Commission should fully exploit its potential to address novel questions raised in respect to data pools and to any other market behaviour inspired by the Big Data revolution.

2.2.3 Recommendation No. 14

Recommendation No. 14

The most appropriate tools to grant legal certainty in questions of anticompetitive behaviour concerning data pooling are:

- the guidelines of the Commission because, by identifying significant circumstances for the application of Article 101 TFEU to data pools agreements, they can be relied upon by undertakings while self-assessing their market behaviours;
- the guidance letters, because the level of change brought about by Big Data in competition law analysis is so massive that genuinely novel questions are likely to arise. This would enable the related applications for guidance letters to be finally upheld by the Commission.

CHAPTER IV: PRIORITY 3 – A EUROPEAN DIGITAL INDUSTRIAL POLICY: SOVEREIGNTY THROUGH COMPETITIVENESS

1 Status quo: A weak European position and a new sentiment

1.1 The EU's position in digital markets

The US and China together account for 75% of global blockchain technologies patents, 50% of global spending in internet of things technologies, more than 75% market share in cloud computing and 90% of the market capitalisation value of the world's 70 largest digital platforms (see also Figure 18).[440]

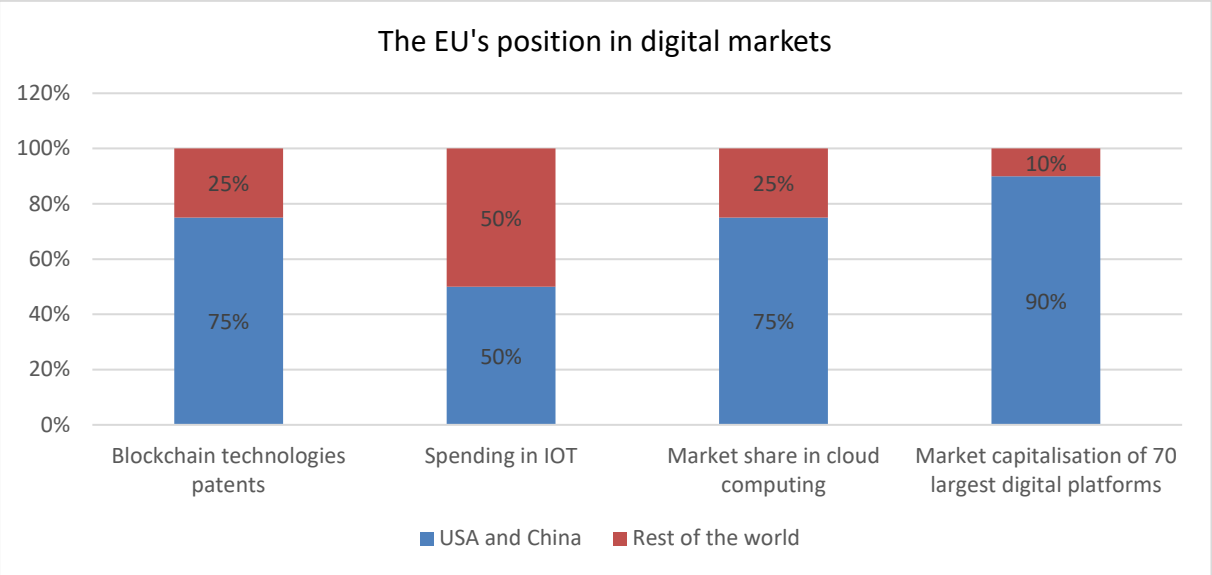

Figure 18: Digital sovereignty
Source: UNCTAD (2019)

What is more, the digital sector is becoming ever more important in recent years. In 2018, the share in the market capitalisation of the world's top 20 companies originated to 56% from companies within the technology and consumer services sector up. In 2009, the share was only 16%.[441] It is estimated that digital technologies like AI, IOT or blockchain could add more than one percentage point of productivity growth year by year.[442] In addition to that, 40% of the more than 4000 colocation data centres worldwide are located in the US.[443] Also, the websites most-used in Western-Europe are originating from the US, which hosts "more than half of the top 100 websites used in 9 of the world's 13 subregions".[444] If looking at mobile operating systems, the Android and the IOS platforms have a reach of 99% in total, with Android being far ahead with a share of 85%. The Chrome browser by the US company Google is the main web browser worldwide accounting for 67% of page-visits. In October 2018, only two European companies – Spotify and Zalando – were part of the 100 top global digital platforms.[445]

440 UNCTAD (2019), p. 2
441 Id. p. 18
442 McKinsey Global Institute (2019), p. 5.
443 Id. p. 12.
444 Id. p. 18.
445 Thieulin (2019), p. 5.

The EU's position in the tech industries is also shown in the EU's overall trade deficit for high-tech products. This deficit stood at 23 billion Euro in 2017, which was mainly due to large imports from China. In this regard, especially imports of electronics communications and computer office machines played a major role.[446]

Despite of that and even though Europe seems to be in a weak position, in some fields, the US and China resort to European expertise. Enterprise software, industrial robotics and even mobile infrastructure and telecom equipment are economic segments, where Europe is (still) one of the front-runners. In robotics, for instance, 8 of the 20 largest companies have their presence in Europe and Nokia and Ericsson still account for more than 30% of global markets in mobile infrastructure deployment.[447]

1.2 Explaining factors

Several factors may offer an explanation for the current situation. We identify three main factors related to (1) the innovative power of the products and services, (2) comparative advantages, (3) the economic characteristics of the platform economy.

(1) The dominant position of the USA and China is, first and foremost, the result of a remarkable number of innovative products and services brought onto the markets in recent years. Without these high-quality, innovative products that found the interest of (European) consumers, the USA and China would not have reached the position they are in today. Consumer goods like the iPhone, the online market place Amazon or the search engine of Google profited from their innovative character.

(2) The EU is a modern, very open economy profiting from free trade with its worldwide partners. The EU accounts for 17,3% of global exports of goods and services. Exports amount to 2875 billion Euro in 2018, more than China with 2344 billion Euro and the US with 2111 billion Euro. Furthermore, the EU-28 hold the same position with respect to global imports of goods and services. Here, its share amounts to 16,1% (US: 15,7% and China: 13,4%).[448] Free trade leads to specialisation where comparative advantages are being played out. This international division of labour is one of the cornerstones of the exchange and the trading of goods and service between countries. An increase in cross-border trading is usually a signal of an increase in the division of labour. Each country specialises in the production of those products and services where it possesses a comparative advantage, while allowing other countries to produce other goods which they can produce in a better and cheaper way. Such specialisation usually serves all participating countries and allows them to focus on their individual strengths.[449] Specialisation always comes with a certain degree of dependency. Countries hence have to rely (to a certain and heterogenous extent) on having access to products and services produced elsewhere when they are not able or willing to produce them at the same quality or at same (opportunity) costs.

The division of labour and specialisation take place heavily in the digital sector, too, where especially the US and China – at least for the time being – are in an advantageous position in many fields – e.g.

446 EU-Commission (2019d), p. 8
447 Id. p. 10.
448 EU-Commission (2019a)
449 Ricardo, David (1891)

cloud computing, 5G, B2C platforms – as compared to other world regions. Those other regions are, thus, regularly dependant on imports from those countries to be able to use them.

(3) Innovative products and services plus comparative advantages are not the only factor explaining the current situation. As stated already in earlier chapters, many digital products and services are characterised by platform features that can help ground-breaking first movers to gain market power more easy as compared to other markets:

- Once having reached a certain critical number of clients, many digital goods, especially those having a platform character, profit from network effects. The value of the service grows with an increasing number of users, making it in turn even more attractive for both new and existing customers.
- Digital goods are also often characterised by high fix costs and low marginal costs. It is regularly expensive to establish a digital platform in the first place, but further expansion through growing user numbers does not lead to high additional costs.
- Network effects may lead to the situation that costumers are unwilling to change to another digital service as switching comes at considerable costs, e.g. the loss of a social network. Thus, lock-in effects strengthen the incumbent.

In many digital markets, US companies have been first movers and have profited from the described advantages this brings about.

In China, the said features also played a main role in the success of digital players such as the BATs (Baidu, Alibaba and Tescent). In this regard, economies of scale are likely to be an important factor for success. In 2016, China had 731 million internet users, which constitute 1,7 times (2,5 times) the number of users in the EU (the US). Considering only mobile internet users, the discrepancy is even larger (2 times and 2,6 times). In addition, the share of Chinese internet users that are defined as being more inclined to the digital sphere ("digital natives") stands at 39% compared to 31% in the EU and 26% in the US. The absolute number of Chinese digital natives is 2,1 times (EU) and 3,8 times (US) higher. (see Figure 19). Consequently the "sheer scale of China's internet base" helped many actors to profit from economies of scale.[450]

[450] McKinsey Global Institute (2017), p. 5.

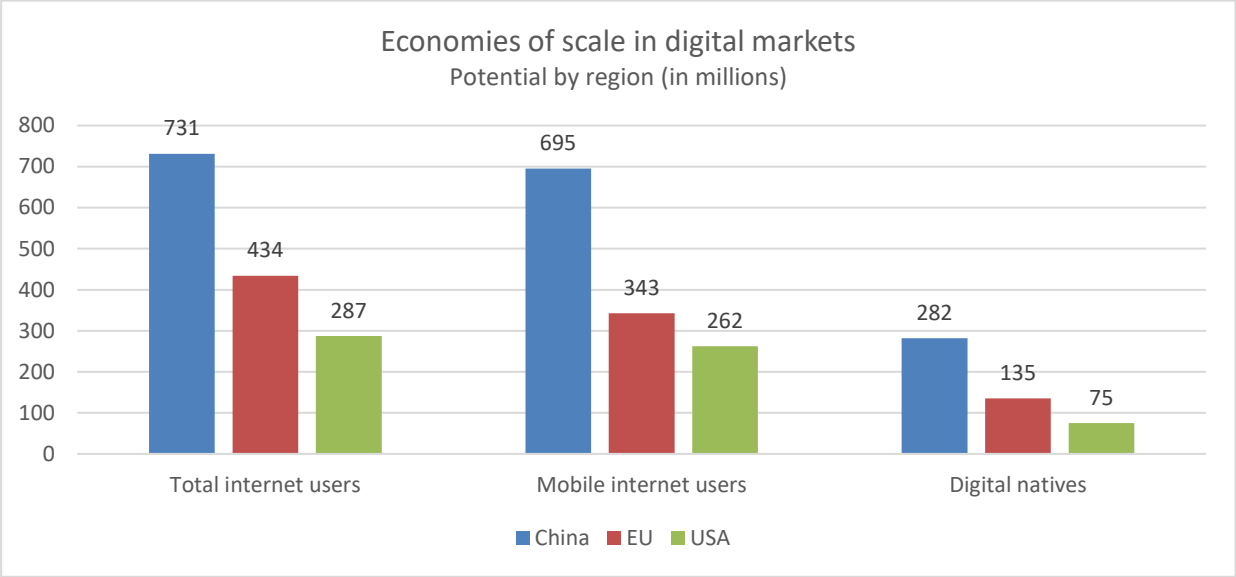

Figure 19: Economies of scale in digital markets, Potential by region, in million
Source: McKinsey Global Institute (2017)

Second, the digital sector in China gained momentum due to access to cheap manufacturing hardware, smartphones and other IT devices produced domestically on which other digital products were and are able to build their products, platforms and services on top.[451] Third, an investment friendly environment plus low regulatory barriers certainly matter. China gave its tech firms a lot of leeway in recent years, basically letting them test and experiment with new products and services without interfering, minor supervision and a low level of consumer protection. What is more, the Chinese public sector also pushed the sector, especially by acting as "investor, innovator and consumer" and provider of funds and tax deductions.[452]

1.3 A new sentiment

The EU's weak position on digital markets has led to increasing calls for political initiative to regain European sovereignty. As President of the EU Commission, Ursula von der Leyen has entrusted the Commissioner for the internal market Thierry Breton with the task "to contribute to the work on enhancing Europe's technological sovereignty. This means investing in the next frontier of technologies, such as blockchain, high-performance computing, algorithms, and data-sharing and data-usage tools. It also means jointly defining standards for 5G networks and new-generation technologies".[453] Furthermore, there are intense discussions on the use third country suppliers' equipment (e.g. Huawei) in the development of digital infrastructure for, in particular, 5G networks.[454] Also, the GAIA-X project for connected data infrastructures recently presented by the German Minister for Economic Affairs and Energy shows growing concerns regarding European cloud capabilities.[455]

This new sentiment finds it origin in mainly two factors:

451 Id. p. 12 and 13.
452 Id. p. 14 and 16.
453 Mission letter, Thierry Breton, Commissioner-designate for Internal Market, EU Commission, November 2019, p. 4.
454 See, e.g. https://www.handelsblatt.com/politik/deutschland/5g-ausbau-bundesregierung-wendet-sich-nun-doch-gegen-huawei/25165694.html?ticket=ST-61045677-ssPX241DVfL493NofOZu-ap3
455 Bundesministerium für Wirtschaft und Energie (2019)

1. **The large economic importance of all things digital:** The whole society, be it consumers, businesses, governments or public bodies is confronted each and every day with digital products and services. As the whole economy seems to get more and more digitalised, not being at the forefront in understanding and handling these developments creates fears.
2. **Political risks which are considered by many to have been increasing in recent years:** The inauguration of the Trump administration in the USA and the policies that followed – e.g. trade conflicts with China and the EU – has caused doubts as to the reliability and trustworthiness of the US policy stance. US regulatory measures such as the US-Cloud Act increased concerns as well that US authorities may access sensible data of European companies stored on the infrastructure of US cloud providers. With respect to China, concerns have grown that the Chinese government may try to incorporate spy instruments in products and services of domestic tech firms that serve the world market and are frontrunner in their specific business sectors (e.g. discussion on 5G deployment and the use of Huawei Technologies Co., Ltd). The uptake of this sentiment of increased political risks translates into concerns of, on the one hand, economic actors within the EU, inter alia, with respect to business secrets or the reliability of existing uninterrupted supply chains. On the other hand, political actors might have concerns related to public interests, e.g. because the functioning of parts of the economy or of public services may be technically dependent upon the political goodwill of third countries.

2 Looking forward: What should be done – 3 Recommendations

Increasing the competitiveness of the European digital economy is the best recipe to strengthen European digital sovereignty. We give a number of recommendations. In the area of cloud-computing, there seem to be convincing reasons for public intervention, although this does not only go back to the EU's dependence upon third-country cloud service providers. In section 0, we design a blueprint for public action in this field.

2.1 Recommendation No. 15: Strengthening the EU's digital competitiveness

Competitiveness is key to being sovereign or less dependent upon suppliers from third countries. The mere fact that a product or service is produced in Europe does not make it attractive to potential users. It must be good, meet consumers preferences and be competitively priced.

Recommendation No. 15

Attaining a competitive European digital economy is a conditio sine que non for digital sovereignty. The bulk of the work and investment to reach this aim has to be delivered by private investors and the private economy. Nevertheless, the EU, national legislators and policy makers should set the appropriate regulatory framework for this to happen. This framework should (1) safeguard the openness of the economy and (2) competition, (3) allow for economies of scale, (4) entail investment friendly infrastructure regulation and (5) promote digital skills.

- **Remaining an open economy and avoid protectionism**

After North America, Western Europe is the most open world region with respect to market access conditions, infrastructure, investment environment, conditions for enterprises and governance as-

pects. The level of openness even increased in recent years, also thanks to several new Free Trade Agreements (FTAs) that the EU concluded e.g. with Canada and South Korea.

The countries that increase their economic openness – e.g. with respect to market access condition, the investment environment (domestic and foreign finance sources finance are widely available), the conditions for enterprises (contestable markets) and governance issues (rule of law, governance integrity) – have a higher productivity.[456] Such productivity gains are decisive in staying competitive in the digital economy. Closing out non-EU competitors in such a manner as to prevent competition does not make life better for Europe as this translates, for instance, into less pressure to innovate and may lead to retaliation.

- **Safeguarding competition**

Recently, there have been several calls for a new European industrial strategy to strengthen the competitiveness of the digital industry. These calls cover topics like "taking into greater consideration the state-control of and subsidies", the "updating of current merger guidelines to take greater account of competition at the global level", the ambition to "become world leaders on Artificial Intelligence and a new "reciprocity mechanism for public procurement with third countries".[457] In general, the political concern that the competitiveness of European industry is at stake is fundamentally appropriate. However, policy action must under no circumstances aim at the public formation of European national champions that threaten to restrict competition in the EU. The preferential award of public contracts to European companies despite higher prices weakens reform incentives in these companies and burdens public budgets. There is a danger that taxpayers' money will be wasted. Europe should instead raise its voice for fair market-based competition that does not favour big EU champions or provides special treatment to a certain group of companies, while discriminating other ones. Only then, a level playing field can be ensured and incentives for urgently necessary innovation are held up.

- **Allowing for economies of scale**

As it has been shown above, economies of scale matter a lot in the digital economy, especially when considering the omnipresence of platforms profiting from network effects. China in particular has a major advantage due to the sheer size of its (digital savvy) population. Since the EU cannot reach the same absolute number of digital users, it is all the more important to allow for economies in scale in the EU to a maximum extent.

We must create a functioning single market for data in the EU that addresses the market barriers resulting from different national rules and lowers the barriers for market entry. This will contribute to reducing the high costs for establishing platform businesses with a critical mass of clients across the EU. This is necessary to allow for network effects and to lower variable costs and will intensify competition to the advantage of European users.

Furthermore, a true digital internal market will contribute to lowering costs of digitalising all economics sectors. The Free Flow of Data Regulation, which requires a less restricted flow of data be-

456 Legatum Institute (2019)

457 German Federal Ministry of Economic Affairs and Energy and French Ministry for the Economy and Finance (2019)

tween EU Member States and bans most of national data localisation requirements, was a good start for further harmonisation.[458] Others should follow suit.

- **Creating investment friendly infrastructure regulation**

Digital markets rely more or less directly on a well-functioning broadband or mobile infrastructure. The existence of such infrastructure is a prerequisite for a prospering digital economy.

In this regard, the EU is not a frontrunner. South-Korea, Japan and the US present a better digital infrastructure that the EU. Canada, Australia and China lag behind, although low population density and geography may distort the picture (see Figure 20).[459,460]In order to encourage investment in the necessary broadband and mobile infrastructure, it is of the utmost importance to create an innovation friendly and stable regulatory framework that allows for intense competition and stimulates investments.

In the EU, access to telecommunications networks from telecoms operators with market power is regulated "ex ante" and certain access fees have been set by national authorities. This approach has been pursued due to the bottleneck character of some elements of the networks, which were deemed essential facilities for competitors.

As useful as ex-ante access regulation may be, it is not an end in itself.

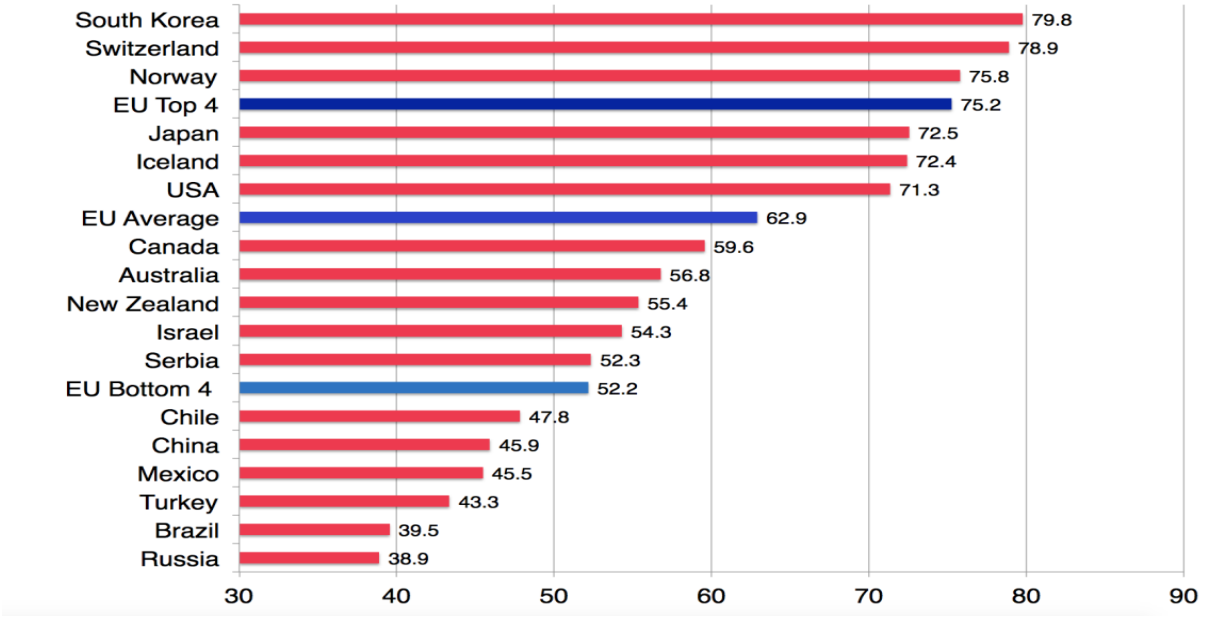

Figure 20: Normalised country scores for the connectivity dimension in 2016
Source: EU-Commission (2018)

It is decisive that such regulation is thoroughly reviewed on a regular basis in order to decide whether there is still a need for it at all. Ultimately, sector-specific ex ante regulation is only appropriate if (1) access to elements of the telecoms network is indispensable for competitors to reach the final customer and thus provide him with his products or services, and (2) such elements cannot be dupli-

458 Hoffmann and Eckhardt (2017)
459 EU-Commission (2018)
460 The figure shows a score which covers seven indicators grouped together in four sub-dimensions that examine fixed and mobile broadband deployment and take-up.

cated. In case duplication is not possible, a natural monopoly may exist, which is not *per se* a sufficient justification for regulation. If a potential competitor can credibly threaten to enter the market, it can discipline the established company to act competitively. In this case, regulation of the monopoly provider is not necessary as markets are contestable. Moreover, technological changes may change the bottleneck character of previously regulated elements – e.g. because of the emergence of substitute products – and access regulation may no longer be necessary. In such a case general competition law is a better and less intrusive instrument to safeguard competition.

Beyond the question whether an access regime is advisable or not, a crucial issue is the stability and predictability of the regulatory environment. Investments in telecommunication infrastructure are usually long-term and tie a huge amount of funds. Frequent changes to the regulatory framework create uncertainties among investors and, thus, inhibit their investments.

- **Promoting digital skills**

In 2018, the EU-27 had 5.8 million data professionals, while the demand for such specialists was at 6,3 million. This lack of skilled workers in the digital economy is unlikely to disappear soon. On the contrary, several projections show that the gap in specialists will further increase. While the gap was at roughly 500.000 people in 2018, scenarios show that it will rise in upcoming years to numbers between 775.000 and 1.551.000 in 2025 (see Figure 21).

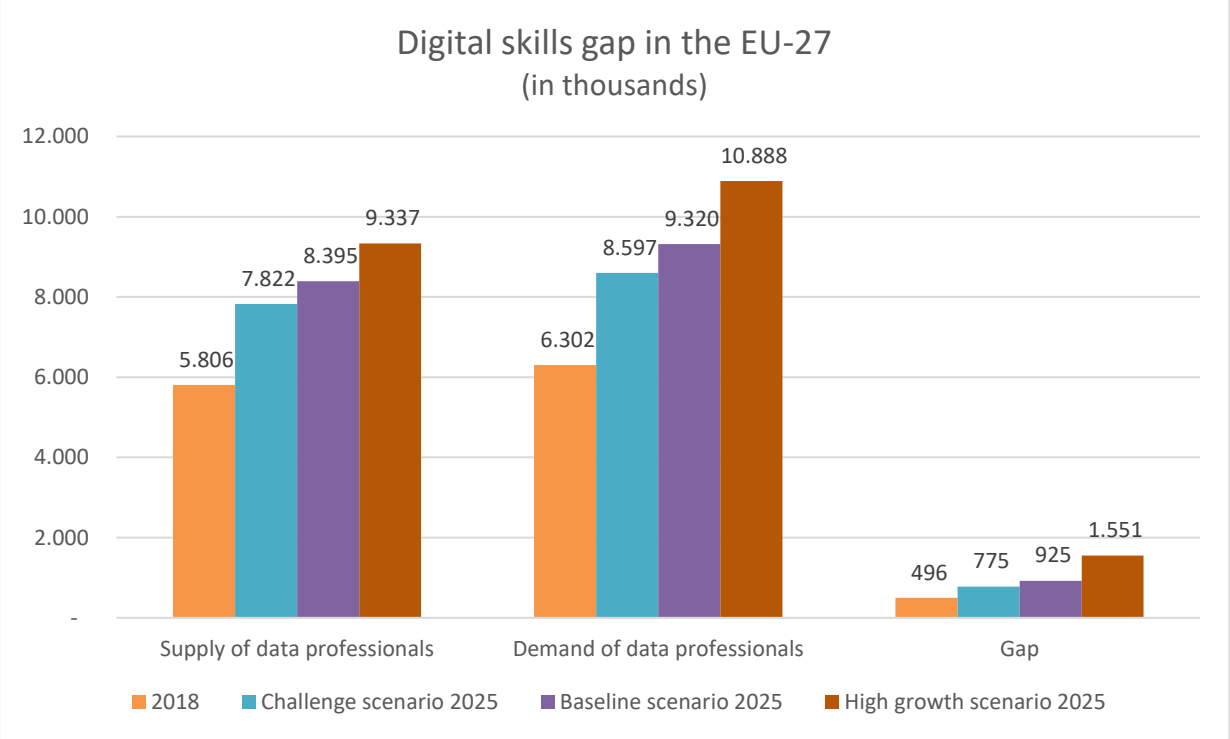

Figure 21: Digital skills gap in the EU-27
Source: International Data Corporation (IDC) and the Lisbon Council (2019)

Even though this figure only depicts the shortage of data professionals, it demonstrates the general necessity to invest in education and training to keep up with other world regions. All claims to enhance Europe's digital sovereignty do not have much value, if skilled workforce is not available to the necessary extent.

Given the EU's limited legal competencies in this field, it is primarily the policy task of Member States to step up efforts for enhanced digital competences.

2.2 Easing tensions in the international datasphere: the GDPR, the US CLOUD Act and conflicts of law

The diffusion of cloud computing – or, more specifically, the subsequent digitisation of many human and business activities that cloud computing enabled - has triggered a number of conflicts of law. Those are due to the fact that the relevant elements to identify the competent jurisdiction and the applicable law could all be located in different legal orders[461].

Looking at this phenomenon from another angle, we can say that digitisation has made regulation of the cloud sector potentially relevant beyond national borders as well as potentially irrelevant within national borders. What is at stake in such litigation is the ability of a legal order to regulate a cross-border operation, thus imposing its values and offering a thorough legal protection to its citizens and to the company based on its territory.

In this sense, it seems important to find a satisfactory solution to the many conflicts of law that cloud computing can raise through appropriate international agreements. This is particularly urgent in the area of cross-border access to data as evidence within criminal proceedings, where, as it will be illustrated, clashes between US and EU law have already materialised.

2.2.1 The US-CLOUD Act

The US Clarifying Lawful Overseas Use of Data Act (CLOUD Act) was signed into law on March 23, 2018 and updated part of the 1986 Stored Communications Act ("SCA"). It regulates the mandated disclosure of electronic communications to the US authorities whenever a probability exists that such communications contain evidence of a crime.[462]

Its aim is to enhance public safety and improve the fight against serious crime.[463] The efficiency of the enforcement authorities in this area has been more and more challenged over time because the internet allows technology companies to store data at a great distance from the physical location of their customers, with the result that electronic communications that provide evidence of a crime often are not housed in the same country where the crime took place. This forces the authorities to seek data stored outside their territorial jurisdiction.[464]

The CLOUD Act addresses this issue, on the one hand, by granting extraterritorial reach to US Government's request to access data stored abroad[465] and, on the other, by establishing a framework for bilateral agreements on cross border data requests by foreign countries.[466] Both aspects will be dealt with in the following pages.

---

461 Woods A.K. (2018), p. 352.

462 The question of whether the US authorities could compel an electronic communications company to release content stored in data centers located out of the US territory was raised in front of the Supreme Court within the case Microsoft Corporation v. United States of America. Following the signature of the CLOUD Act and the obtention of a warrant by US authorities under the authority of the new law, however, the case was dismissed as moot. See No. 17-2, 548 U.S. __, 2018 WL 1800369, slip op. at 2 (U.S. Apr. 17, 2018) (per curiam) (vacating and remanding with instructions to dismiss as moot).

463 CLOUD Act § 102 (2); codified at 18 U.S.C. § 2713

464 Mulligan S.P. (2018)

465 CLOUD Act § 103(a)(1); codified at 18 U.S.C. § 2713

466 CLOUD Act § 105; codified at 18 U.S.C. § 2523

2.2.1.1 The extraterritorial reach of US-based mandatory disclosure warrants

The CLOUD Act enables the United States Government to access data that is in the custody, control, or possession of communications service providers, which are subject to the jurisdiction of the United States, regardless of whether such data is inside the United States.[467]

The latter provision is complemented by a set of rules designed to prevent conflicts of law that could emerge whenever the law of the country where data is stored prohibits such disclosure. Notably, the CLOUD Act prescribes that an applicant can ask for a warrant to get access to data abroad to be quashed or modified when (a) the provider reasonably believes that the communication content concerns a non-US citizen[468] residing out of the US and (b) the provider reasonably believes that the disclosure of such data would probably violate the laws of a qualifying foreign government[469], i.e. a government with which the US have an agreement on data exchange. The Court may decide to uphold the application (1) when the disclosure would violate foreign law, (2) when the interest of justice, as it emerges from the totality of relevant circumstances, demands the warrant to be quashed or changed and (3) when the warrant concerns a non-US citizen residing out of the US.[470] Compliance with the condition under (2) must be assessed through a "comity analysis".

Comity is a common law doctrine that, "*among other things, permits courts to excuse violations of U.S. law, or moderate the sanctions imposed for such violations, when the violations are compelled by a foreign nation's law*".[471] The CLOUD Act enshrines this doctrine in concrete legal provisions, thus providing legal clarity as to the factors that the court might take into account when considering whether to quash or modify the data access warrant.[472]

If the application of the above legal regime is insufficient to neutralise conflicts of law, the Department of Justice suggested in its White Paper that "*the U.S. government could elect to pursue alternate channels, such as narrowing or modifying a request to avoid the conflict; resolving the conflict through closer inquiry or good-faith negotiation; or making the request under an applicable* [Mutual Legal assistance Treaty (MLAT)]"[473]. However, "[s]*hould the U.S. government seek to enforce the order notwithstanding a conflict with foreign law, U.S. courts can be expected to apply long-standing U.S. and international principles regarding conflicts of law to ensure appropriate respect for interna-*

467 CLOUD Act § 103(a)(1); codified at 18 U.S.C. § 2713

468 "United States person" under the CLOUD Act is a citizen or national of the United States, an alien lawfully admitted for permanent residence, an unincorporated business association in which a substantial number of members are citizens or lawfully admitted permanent residents, or a corporation that is incorporated in the United States. See CLOUD Act § 105(a) codified 18 U.S.C. § 2523(a)(2).

469 CLOUD Act § 103(b) codified at 18 U.S.C. § 2703(h)

470 CLOUD Act § 103(b) codified at 18 U.S.C. § 2703(h)

471 Mulligan S.P. (2018), p. 9

472 The CLOUD Act lists the factors that the court "shall take into account, as appropriate[,] in its comity analysis: (A) the United States' interests; (B) the foreign governments' interests; (C) the likelihood, extent, nature and penalties that the provider or its employees could face under foreign law; (D) the location and nationality of the target of the demand, and the nature and extent of the target's connections with the United States and the foreign nation; (E) the nature and extent of the provider's ties to and presence in the United States; (F) the importance of the information to the investigation to be disclosed; (G) the ability to access the information through other means; and (H) the investigative interests of the foreign nation if the data is sought by the United States on behalf of a foreign nation". See CLOUD Act § 103(b) (adding 18 U.S.C. § 2703(h)(3)).

473 U.S. Department of Justice (2019), p. 16

tional comity by applying a multi-factor balancing test, taking into account the interests of both the United States and the foreign country".[474]

2.2.1.2 Bilateral agreements under the US CLOUD Act

While foreign authorities often seek access to data held by companies based in the US, before the entry into force of the CLOUD Act, service providers were not allowed under US law to comply with foreign mandatory disclosure orders, with two notable exceptions: i) a statutory provision expressly allowing the company to do so ; ii) a warrant issued by a federal court.[475] Lacking an internal legal framework comprehensively addressing the issue, foreign authorities could still rely on letters rogatory[476] and Mutual Legal Assistance Treaties (MLATs), neither of whom was considered a truly expedite instrument for cross-border evidence sharing.[477] The problem was exacerbated by the fact that "*the vast majority of the world's Internet users store their data with U.S. firms*".[478]

The CLOUD Act now authorises the United States to enter into executive agreements for sharing evidence with countries that meet specific requirements. More specifically, the legislation "*authorizes executive agreements that lift any restrictions under U.S. law on companies disclosing electronic data directly to foreign authorities for covered orders in investigations of serious crime. This would permit U.S.-based global* [communications service providers] *to respond directly to foreign legal process in many circumstances*".[479] The only legal effect of such CLOUD agreements is therefore "*to eliminate the legal conflict for qualifying orders*".[480]

At the same time, the CLOUD Act details the characteristics that a legal order must possess for the US to negotiate an agreement with the related government. First, the negotiating partner must have in place "*robust substantive and procedural protections for privacy and civil liberties*".[481] These protections include procedural laws on cybercrime and electronic evidence, respect for the rule of law and universal human rights – e.g. fair trial and freedom of expression –, and the clarity of the legal mandates and procedures governing the foreign entities authorised to access data.[482] Secondly, the foreign government concerned by the executive agreement must have "*appropriate procedures to minimise the acquisition, retention, and dissemination*"[483] of data relating to US persons.

Also, the CLOUD Act establishes additional significant requirements for the evidence disclosure order to be covered by the agreement. The order issued by the foreign government shall inter alia be in relation to "*the prevention, detection, investigation, or prosecution of serious crime*"[484], identify a specific person and specific identifiers such as an address, and comply with the domestic law.[485]

474 U.S. Department of Justice (2019), p. 16
475 Mulligan S.P. (2018), pp. 10 – 11
476 "Discretionary requests made between the courts of one country to the courts of another country that are available to governments and private litigants, which are generally seen as the least efficient and reliable method of obtaining evidence abroad" (Mulligan S.P. (2018), p. 11).
477 "Treaties providing streamlined processes for cross-border evidence sharing between governments in criminal cases, which are reviewed by DOJ and a federal court for compliance with U.S. law" (Mulligan (2018), p. 11).
478 Woods A.K. (2016)
479 U.S. Department of Justice (2019), p. 4
480 U.S. Department of Justice (2019), p. 5
481 CLOUD Act § 105; codified at 18 U.S.C. § 2523 (b) (1)
482 CLOUD Act § 105; codified at 18 U.S.C. § 2523 (b) (1) (B)
483 CLOUD Act § 105; codified at 18 U.S.C. § 2523 (b) (2)
484 CLOUD Act § 105; codified at 18 U.S.C. § 2523 (b) (3) (D) (i)
485 CLOUD Act § 105; codified at 18 U.S.C. § 2523 (b) (3) (D)

The bilateral executive agreement must require from the foreign government not to intentionally target a US person[486] or a person located in the US, or to target a non-US person to get information on a US person.[487]

Among the other requirements, the foreign government shall also remove restrictions to disclose data on service providers – including the ones subject to US jurisdiction – in order to allow reciprocal rights regarding data access.[488] The first executive agreement concluded in relation to the CLOUD Act is the *Agreement between the UK and the US on Access to Electronic Data for the Purpose of Countering Serious Crime of 3 October 2019* (UK-US Agreement).

It must be noted that the UK-US agreement prevents UK authorities from accessing data from US persons but US authorities can access data of UK persons. The agreement therefore lacks reciprocity regarding the exclusion of persons that can be targeted by foreign authorities.

Communications service providers remain however subject to legal obligations to produce data pursuant to UK or US law.[489] This implies that the first prong of the CLOUD Act which allows US authorities to access data held by service providers subject to US jurisdiction continues to be applicable. The same goes for provisions of the UK regulating access to data by UK authorities. While a bilateral data-sharing agreement can be expected to establish clear rules and a framework of access to data by the national authorities concerned, UK and US authorities could actually avoid limitations and safeguards provided in the agreement by applying national law.[490] This subordination of the UK-US agreement to national laws leads to legal uncertainty and the agreement therefore does not prevent conflicts of law.

2.2.1.3 The problem of conflicting legal obligations stemming from the GDPR and the CLOUD Act

The extraterritorial reach of warrants to access data under the current US legal framework raises the issue of whether service providers controlling such data, which are subject to EU law, can be exposed to conflicting laws. Namely, the data transfer required by US warrants qualifies as processing and falls as such under the GDPR.

Article 48 GDPR specifically considers transfers of personal data ordered by judicial or administrative authorities of third countries like the US. According to this provision, "[a]ny judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State".

Recital 115 highlights that "the extraterritorial application of those laws, regulations and other legal acts which purport to directly regulate data processing under the jurisdiction of the Member States

---

486 A US person is (1) a US citizen or national, (2) a person having lawful permanent residence in the US, (3) an unincorporated association composed of a majority of members from the first 2 categories, or (4) a corporation that is incorporated in the US. See CLOUD Act § 105; codified at 18 U.S.C. § 2523 (a) (2).

487 CLOUD Act § 105; codified at 18 U.S.C. § 2523 (b) (3) (A) and (B)

488 CLOUD Act § 105; codified at 18 U.S.C. § 2523 (b) (3) (I)

489 UK-US Agreement, Art. 6 (3): „This Agreement does not in any way restrict or eliminate any legal obligation Covered Providers have to produce data in response to Legal Process issued pursuant to the law of the Issuing Party."

490 Christakis T. (2019), pp. 6-7

may be in breach of international law and may impede the attainment of the protection of natural persons ensured in the Union by the GDPR". Accordingly, "transfers should only be allowed where the conditions of this Regulation for a transfer to third countries are met".[491]

The above provisions of the GDPR clearly rule out that a request from a foreign authority constitutes a legal ground for transfer *per se*[492].

When an appropriate agreement is in place, the order issued in the third country is enforceable under EU/the Member State's law. However, "*EU companies should generally refuse direct requests and refer the requesting third country authority to an existing mutual legal assistance treaty or agreement*".[493]

When, instead, no international agreement is in place, the order will have no legal value under EU/the Member State's law. A conflict of law can therefore materialise.

In a recently delivered legal opinion upon request of the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE), the European Data Protection Supervisor (EDPS) and the European Data Protection Board (EDPB) suggest that the legitimacy of a data disclosure or data transfer in compliance with a third country's warrant by a service provider subject to EU law should be reviewed according to the following legal test: first, it should be ascertained whether such processing can rely on one of the legal basis listed under Article 6 GDPR; then, if this is the case, the interpreter should test the applicability of one of the exceptional grounds for processing mentioned by Article 49 GDPR.[494] Only the joint presence of such legal justifications on a case by case basis can ensure the legality of the cross-border data processing towards the third country when it is not authorised under EU or a Member State's law.

---

491 "This may be the case, inter alia, where disclosure is necessary for an important ground of public interest recognised in Union or Member State law to which the controller is subject" (GDPR, Recital n 115).

492 See European Commission's Amicus Curiae brief in USA v. Microsoft corporation p. 14, accessible at https://www.supremecourt.gov/DocketPDF/17/17-2/23655/20171213123137791_17-2%20ac%20European%20Commission%20for%20filing.pdf

493 "The EDPB therefore reiterates its position expressed in its guidelines on Article 49 GDPR that: "In situations where there is an international agreement such as a mutual legal assistance treaty (MLAT), EU companies should generally refuse direct requests and refer the requesting third country authority to an existing mutual legal assistance treaty or agreement". Indeed, we consider that where disclosure of personal data is compelled by a third-country authority, the MLAT process must ensure that data is disclosed in compliance with EU law, and under the supervision of the courts in the EU" (EPDB-EDPS Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection, ANNEX, 12 July 2019, p. 3).

494 Under Article 49 (1) GDPR, "a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions: (a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards; (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request; (c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person; (d) the transfer is necessary for important reasons of public interest; (e) the transfer is necessary for the establishment, exercise or defence of legal claims; (f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; (g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case".

However, "*the EDPB and the EDPS consider that an international agreement containing strong procedural and substantive fundamental rights safeguards appears the most appropriate instrument to ensure the necessary level of protection for EU data subjects and legal certainty for businesses*".[495]

2.2.2 Recommendation No. 16: A US-EU agreement that protects EU citizens and EU-based companies

In order to clearly frame requests for direct access to data by judicial authorities and to ensure the necessary safeguards, the EU should negotiate an agreement with the US.

An EU-US Mutual Legal Assistance Treaty (MLAT) has already been signed in 2009 to regulate evidence sharing in criminal matters.[496] It complements bilateral MLATs concluded between EU Member States and the US.

The Commission has recently adopted a Recommendation for a Council Decision to authorise the opening of negotiations in view of an international agreement between the EU and the US on cross-border access to electronic evidence for judicial cooperation in criminal matters and negotiating directives.[497] On 6 June 2019, the Council adopted the recommended Decision.[498] The Council fixed a few guidelines that the Commission is to comply with in the context of the negotiation.[499]

First, the Commission should achieve the following objectives: address conflicts of law and set common rules regarding judicial authorities' orders for obtaining electronic evidence from service providers, allow for a direct transfer of electronic evidence on a reciprocal basis, and ensure respect for fundamental rights and principles.[500]

Secondly, the nature and scope of the agreement should be clearly defined. The agreement should *inter alia* define the criminal proceedings (both pre-trial and trial phases), the types of data and the criminal offences and thresholds it applies to.[501] It should also include reciprocal rights and obligations, effective judicial remedies for data subjects and a service providers' right to object to an order.[502]

Thirdly, the agreement should make applicable by reference the EU-U.S. Data Protection and Privacy Agreement ("Umbrella Agreement")[503], already in force, while at the same time complementing it with additional safeguards. The inclusion of additional safeguards is motivated by the necessity to

---

495 EPDB-EDPS Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection, ANNEX, 12 July 2019, p. 8.

496 Council Decision 2009/820/CFSP of 23 October 2009 on the conclusion on behalf of the European Union of the Agreement on extradition between the European Union and the United States of America and the Agreement on mutual legal assistance between the European Union and the United States of America

497 EU-Commission (2019b)

498 Council Decision authorising the opening of negotiations with a view to concluding an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters.

499 Council Addendum to the Recommendation for a Council Decision authorising the opening of negotiations with a view to concluding an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters ("Addendum to Council Decision on the EU-US agreement negotiations")

500 Addendum to Council Decision on the EU-US agreement negotiations, pp. 2-3

501 Addendum to Council Decision on the EU-US agreement negotiations, p. 3

502 Addendum to Council Decision on the EU-US agreement negotiations, p. 3

503 Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences

address greater personal data protection and procedural rights protection concerns than the general Umbrella Agreement. Notably, such safeguards should adequately reflect (i) the sensitivity of the categories of data concerned (i.e. relating to a criminal proceeding) and (ii) the fact the transfer of electronic evidence directly by service providers rather than between authorities[504]. For example, the decision underlines that the agreement should define the purposes for which personal data and electronic communications data may be requested and transferred, and that the order requesting them should only do so in so far as their access is necessary and proportionate in relation to the stated purpose[505].

Recommendation No. 16

The EU, through the Commission, should negotiate an agreement with the US, which clarifies the rules regarding cross-border access to electronic evidence in the context of criminal proceedings. Not only should this agreement protect EU citizens and companies by ensuring the necessary safeguards, but it should also aim at increasing legal certainty in data access requests by US judicial authorities to EU service providers, thus preventing conflicts of law.

2.3 Recommendation No. 17: A blueprint for public action in cloud computing

2.3.1 Justification for public intervention

Business users and public administrations in Europe are still hesitant to adopt cloud computing. Concerns relate to data security, GDPR compliance, data portability and data governance, i.e. to what extent users can control who will have access sensitive data in the cloud. The dependency on non-European cloud infrastructure providers has increased these concerns.

In fact, the predominant use of non-European cloud services has sparked a discussion on the need for public intervention. However, it is necessary to clearly distinguish between two risks associated with the use of non-European cloud infrastructure:

- Corporate users' main concerns associated with the intensive use on non-European cloud providers seem related to intellectual property concerns and business secrets. Given the US-Cloud-Act and general political risks, the security of corporate data on non-European cloud infrastructure may be found suboptimal. It is up to the individual corporate user to assess whether this danger is present and substantial. If yes, corporate management may limit the use of third-country providers in certain areas of its business. As the costs of any risk materialising are primarily concentrated with the corporate user, there is no compelling policy argument for public intervention.
- There is a political risk that intervention by third countries' administrations may negatively impact the ongoing availability of third country providers' cloud services in the European Union. The lack of such availability may have severe negative impacts both for the company concerned, but also for the EU as a whole. Note that an availability-risk may also occur when using EU-based cloud service providers. In that context however, the risk is of an operational nature, not of a political one.

504 Addendum to Council Decision on the EU-US agreement negotiations, p. 2
505 Addendum to Council Decision on the EU-US agreement negotiations, p. 2

The company concerned may in many cases have a self-interest in guaranteeing ongoing availability of its services to avoid reputational damage. This goes e.g. for banks or utility companies, as customers will not value blocked bank accounts or inactive heating systems. However, companies may assess the political risk very differently and at the same time, it may be difficult for non-professional users to monitor which cloud infrastructure is actually being used.

The negative consequences of a lack of availability of services because of political and operation risks may not be limited to the supplier and its direct users. In some cases, negative externalities may occur. This may be the case when:

- The lack of availability affects a **public good**. As an example, the individual risk-assessment of a bank may result in the bank continuing to use non-EU cloud infrastructure. This may be a rational decision both for the bank and for its customers. However, upon the risk materialising, the negative consequences of the bank being unable to offer its services may have negative consequences for (the customers of) other banks. Liquidity shortfalls may arise and bank transfers to customers of other banks may no longer be possible. These consequences may be far-reaching and affect financial stability as a whole. Obviously, the bank management may not have an economic reason to take these costs into account when making its initial risk assessment.[506]
- **Competition** may be absent or too low. If users have no alternative to using the services of a given supplier, they cannot express their preference regarding the continuity of supply and the subsequent quality of cloud services used by the supplier. At the same time, the supplier will likely underestimate the costs of non-availability of his services and will underinvest in this availability.
- The costs of the lack of availability may be **prohibitively high**. There may be use cases where the lack of availability of services may have far-reaching consequences for public order or for human health and may decide between life and death. In such cases, it may be found inadmissible for private actors to come to an individual assessment of the risk of non-availability of its services.

In these cases, the non-availability risks emanating from political risks associated with the use of third-country cloud infrastructure may require public intervention. The same reasoning goes for non-availability as operational risk emanating from European (and non-European) cloud service providers. This availability may have the character of a public good or its lacking may be associated with such high costs that a “public interest” is present, justifying public intervention regarding the use of cloud service infrastructure. However, even in this case, any public intervention must be as proportionate, efficient and non-discrimination as possible.

The following establishes a framework for such intervention.

2.3.2 An EU framework for secure and trusted cloud computing

We propose the creation of an EU framework for secure and trusted cloud computing in a three-step approach. Step 1 entails defining requirements for secure and trusted cloud computing. In essence this means establishing cloud security certification schemes which may differ according to the speci-

506 Similar problems may arise regarding the continuity of supply of other critical services, e.g. energy or electricity.

ficities of the economic user of the cloud infrastructure. Step 2 entails the actual certification of an applying cloud service supplier. In step 3, we propose a uniform application of regulatory requirements aiming at selected economic operators as to the security standard of cloud services used.

2.3.2.1 Step 1: Defining Cloud Security Certification Schemes

In a first step, the EU should define common requirements for secure and trusted cloud computing by addressing concerns related to data security, data governance and service availability in the cloud. Cloud Security Certification Schemes are instrumental to address these concerns. The existing EU-Cybersecurity Act may serve as a mechanism for setting those schemes. Other relevant topics, such as data portability and GDPR compliance in the cloud may also be dealt with (see box 5).

2.3.2.1.1 Certification schemes in the EU Cybersecurity Act

In April 2019 the EU Cybersecurity Act [Regulation (EU) 2019/881] entered into force. The Regulation includes a framework for the establishment of European cybersecurity certification schemes. Its purpose is to ensure an adequate level of cybersecurity for ICT products, services and processes in the EU.[507] ICT products, services and processes evaluated under such schemes have to comply with specified security requirements. These requirements shall protect "the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the functions or services offered by, or accessible via, those products, services and processes throughout their life cycle".[508] The non-availability risks (be them purely operational risks or also political risks) that have been identified above as a justification for public intervention are thus covered by the security objectives of the cybersecurity certification schemes.

The European Union Agency for Cybersecurity (ENISA) is the responsible EU agency for developing such certification schemes.[509] As a rule, ENISA will develop such a scheme for a certain ICT product, service or process only when mentioned in a rolling work programme that the EU Commission publishes at least every three years[510] and only if the EU Commission instructs the ENISA to develop the scheme. The Commission is still preparing the first version of its rolling working programme and will conduct a consultation on the programme.[511] Only in "duly justified cases", the Commission as well as the European Cybersecurity Certification Group (ECCG)[512] can demand the ENISA to prepare a specific certification scheme without it being included in the current work programme.[513] On December 9 2019, the Commission has tasked the ENISA with preparing a cybersecurity certification candidate scheme for cloud services.[514]

Each certification scheme developed by ENISA has to fulfil several security objectives. It must, inter alia "protect stored, transmitted or otherwise processed data against accidental or unauthorised storage, processing, access or disclosure" and ensure "that authorised persons, programs or ma-

507 Art. 2, Regulation (EU) 2019/881
508 Art. 46 (2) and Art. 51, Regulation (EU) 2019/881
509 Art. 49, Regulation (EU) 2019/881
510 The first rolling work programme must be published by the Commission by 2 June 2020 at the latest. [Art. 47 (5), Regulation (EU) 2019/881]
511 https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-act-brings-strong-agency-cybersecurity-and-eu-wide-rules-cybersecurity
512 The ECCG is a group composed of representatives of national cybersecurity certification authorities or representatives of other relevant national authorities [Art. 62, Regulation (EU) 2019/881].
513 Art. 47 (5) and Art. 48, Regulation (EU) 2019/881
514 https://ec.europa.eu/digital-single-market/en/news/towards-more-secure-and-trusted-cloud-europe

chines are able only to access the data, services or functions to which their access rights refer".[515] Furthermore, for each scheme one or more "assurance levels" – 'basic', 'substantial' or/and 'high' – need to be defined, dependant on the "level of the risk associated with the intended use of the ICT product, ICT service or ICT process, in terms of the probability and impact of an incident".[516] Any certification scheme developed by ENISA becomes applicable only after being adopted by means of an implementing act by the Commission.[517]

2.3.2.1.2 The CSPCERT WG-proposal for cloud security certification schemes

Meanwhile, the Cloud Service Provider Certification Working Group (CSPCERT WG) has been established in December 2017 to discuss an EU certification scheme for cloud computing services. The Working Group published its recommendations to the Commission in June 2019.[518] In its recommendations, the CSPCERT WG advised the Commission to include a cloud services certification scheme in the next rolling working programme and to instruct ENISA to develop such a certification scheme.[519] The CSPCERT WG recommends – in compliance with the Cybersecurity Act – three different assurance levels for cloud computing: basic, substantial and high. It further suggests that such scheme should provide for "sufficiently clear guidance on which assurance level should be linked to which potential Personal/Business/Societal risk scenario impacts", add clarifications as to what the different levels indicate and provide examples as to which assurance level may be appropriate for which services. Also, the CSPCERT WG recommends that an EU cloud certification scheme should allow for "added Security Objectives in addition to the existing certification", e.g. for a specific sector.[520]

2.3.2.1.3 EU cloud security certification schemes

In December 2019, the EU-Commission has mandated ENISA with proposing a cloud computing certification scheme. As part of its mandate to propose a cloud security certification scheme under the European Cybersecurity Certification Framework, ENISA should develop

- a general certification scheme for cloud computing in all economic sectors. In fact, in December 2019 the European Commission has asked ENISA to develop such as scheme.
- sector-specific schemes for seven sectors which are identified in the NIS-Directive (energy, transport, banking, financial market infrastructure, health sector, drinking water supply and distribution and digital infrastructure) and the sub-sectors of those sectors and a specific scheme for cloud computing by public administrations, similar to USFEDRAMP and UK Gov Cloud (see Box 4 below).

Whereas the general cloud security certification scheme should be limited to adherence with general European regulation, when drafting sector-specific additions, ENISA and the regulators of the relevant sectors[521] should meet in joint committees. This cooperation will be necessary to ensure that

515 Art. 51, Regulation (EU) 2019/881
516 Art. 52 (1), Regulation (EU) 2019/881
517 Art. 49 (7), Regulation (EU) 2019/881
518 Online at: https://drive.google.com/file/d/1J2NJt-mk2iF_ewhPNnhTywpo0zOVcY8J/view
519 CSPCERT WG (Milestone 3) Recommendations for the implementation of the CSP Certification scheme, June 2019
520 Recommendations for the implementation of the CSP Certification scheme, p. 22-27
521 For the financial sector, these regulators would comprise of EBA (European Banking Authority) and the ECB (European Central Bank) for banks, EIOPA (European Insurance and Occupational Pensions Authority) for insurances and ESMA (European Securities and Markets Authority) for investment firms. For the energy sector, ACER (The European Union Agency for the Cooperation of Energy Regulators) would be involved.

sector-specific relevant elements of cloud security can be adequately identified and taken into account. Decision making in the joint committees should require a qualified majority in both committees.

Both the general and each of the sector-specific additions should set out three assurance levels, ranging from "basic" and "substantial" to "high". This approach is necessary to guarantee the risk-based approach correctly chosen by the EU Cybersecurity Act. As foreseen in the Cybersecurity Act, the assurance level shall be commensurate with the level of the risk associated with the intended use of the ICT product, ICT service or ICT process, in terms of the probability and impact of an incident.[522]

It is important to remind that standards for certifications schemes for economic activities should be set at the EU-level, in order to avoid distortions in competition in the internal market. It should be avoided that companies (e.g. banks) which originate from different Member States but are competing against each other are subject to different certification schemes. Harmonised standards for certification schemes are a condition-sine-qua-non to avoid such distortion. A second condition is the harmonised application of the schemes to economic activities (see Step 3 below).

Public administrations are neither profit-oriented nor are they competing with other administrations. However, common certification standards will increase data exchange between administrations as well as between administrations and users of public data. Moreover, common standards may enable economies of scale when cloud service suppliers do not have to apply for certification according to different national standards. This may lower cloud costs for administrations as well.

The US FedRAMP program

The Federal Risk and Authorisation program (FedRAMP) was implemented by the US government to provide for a "standardized approach to security assessment, authorisation, and continuous monitoring of cloud-based services".[523] FedRAMP has been implemented in 2011[524] and is based on the Federal Information Security Modernisation Act (FISMA)of 2002.[525] FISMA stipulates for "each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and systems that support the operations and assets of the agency".[526]

The aim of the FedRAMP program was to implement the "Cloud First" policy approach that was presented by the Office of Management and Budget (OMB) at the end of 2010, which sets a duty on all federal agencies in the US to use cloud-based services as long as "a secure, reliable, cost-effective cloud option exists". All Federal Agency that want to use cloud service were obliged to follow the FedRAMP requirements by June 2014.[527]

FedRAMP provides for standardised security requirements for the authorisation of cloud services and their cybersecurity, based on different information system impact levels. Cloud service providers that want to offer their services to federal agencies must fulfil the FedRAMP security requirements and must undertake regular security controls. FedRAMP also includes third-party assessments of security controls implemented by the cloud service providers. Those third-party conformity assessors provide

522 Art. 52(1), Regulation (EU) 2019/88
523 FedRAMP (2017)
524 Id, p. 3
525 Id, p. 2
526 Risk Management, FISMA Background, NIST, available at: https://csrc.nist.gov/projects/risk-management/detailed-overview
527 FedRAMP (2017), p. 2 and 3

for an analysis of the overall risk posture of a cloud service, which serves as a basis for an authorisation process of the cloud service provider that want to establish a business relationship with Government bodies.[528,529,530]

The UK GOV cloud

Similar to the US, the United Kingdom decided in 2011 to implement a Cloud First Strategy for the public sector to support a shift from on premise IT infrastructure to cloud-based services. This included the establishment of a framework for cloud procurement to government departments and public agencies (the G-Cloud framework) and a marketplace, which entails a list of pre-approved cloud service providers and the service they offer (hosted on the Digital Marketplace).[531]

The G-Cloud framework has been installed to streamline procurement processes for public bodies that want to use cloud services.[532] Cloud service providers must go through a process, primarily based on vendor self-declarations, to become a member of the G-Cloud and be listed in the Digital Marketplace.[533] The G-cloud framework shows three classification levels – Official, Secret and Top Secret.[534] The self-certification includes a declaration against the National Cyber Security Centre's 14 "cloud security principles" at the "Official" level. The "cloud security principles" cover, i.a., the security, governance and management processes.[535] Self-certification statements allow cloud service providers to enter the Digital Market Place. Public bodies that want to use cloud services can select between those providers based on their specific security requirements.[536]

Box 4: Public cloud programmes in the USA and UK

Data protection and data portability in the cloud

Whereas the cyber security act as the legal basis for cloud security certification schemes does not make an explicit reference to **data protection** under the GDPR as an element of certification schemes, it does include the protection of data against unauthorised processing as potential objective of the schemes. At the same time, Article 40 of the GDPR calls upon the Commission to encourage the drawing up by industry of codes of conduct regarding the application of the GDPR (here:) to cloud services. Such industry codes of conduct may – if found by data protection supervision authorities to be in compliance with the GDPR – be declared legally binding to all cloud providers by the EU-Commission.[537]

528 FedRAMP (2011)

529 James Sanders and Brandon Vigliarolo (2019), The top cloud providers for government, August 2019, available at: https://www.zdnet.com/article/the-top-cloud-providers-for-government/

530 FedRAMP (2017), p. 2 and 3.

531 Bonneau V. and Mahieu B. (2013)

532 Id, p. 10.

533 United Kingdom Government-Cloud (G-Cloud) OFFICIAL, Microsoft, available at: https://www.microsoft.com/en-us/TrustCenter/Compliance/UK-G-Cloud

534 Clouds in the category „Official" mostly cover public clouds, community clouds and hybrid clouds. Clouds in the "Secret" and "Top Secret" category are usually private clouds or small community clouds.

535 Cloud services and the government security classification policy, White paper, Skyscape cloud services.

536 The G-Cloud Security Approach, Digital Marketplace blog, June 2014, available at: https://digitalmarketplace.blog.gov.uk/2014/06/09/the-g-cloud-security-approach/

537 The Commission will do so be adopting an implementing act, which is subject to review by Member States and the European Parliament, Art. 40 (9) GDPR

In April 2019, the EU Cloud Code of Conduct General Assembly has transmitted a draft EU Cloud Code of Conduct (EU cloud CoC), which specifies data protection obligations.[538] Depending on the endorsement by supervisor and whether the Commission will use its powers, the EU Cloud CoC may hence become legally binding. If so, there is no added value to incorporate the EU cloud CoC into the cloud certification scheme as it will have to be respected in any way.

Data portability is directly addressed in the EU free flow of data Regulation [EU2018/1807]. According to the regulation, the Commission shall "encourage and facilitate the development of self-regulatory codes of conducts" regarding data portability. The codes of conduct are to ascertain that professional users can make informed choices regarding the use of cloud services and the conditions for porting data after termination a contract. The focus of the codes is hence on information and operational requirements. According to the regulation, the Commission shall encourage the effective implementation of the codes of conduct by 29 May 2020.[539] Different from the data protection codes of conduct under the GDPR, there is no procedure enabling the Commission to declare the code(s) to be legally binding.[540]

As data portability is no objective of the security certification schemes in the cyber security act, the data portability code(s) of conduct cannot be included in the certification schemes. Notwithstanding, the Commission may encourage their implementation of may address the importance of portability when applying EU competition law (see Recommendation No. 13)

Box 5: Data protection and data portability in the cloud

2.3.2.2 Step 2: Certification of cloud service suppliers

For the cloud security certification schemes outlined above, the EU Cybersecurity act already governs the certification of the cybersecurity of a certain ICT product, service or process, for which a scheme has been developed. Certification is voluntary for the providers of said product, service or process unless European or national law prescribes otherwise.[541] The Commission will assess at least every second year and for the first time by end of 2023 whether an EU law should make selected certification schemes compulsory.[542]

The existing modalities for the issuing of certificates in the Cybersecurity Act can be applied to the certification of cloud service suppliers without any change. Hence, certificates may be issued by conformity assessment bodies, which are accredited by national accreditation bodies. However, when a high assurance level is foreseen under a certain scheme, in general, the national cybersecurity certification authority is responsible, unless it delegates the task to a conformity assessment body.[543]

We see no need for making certification compulsory. Certification will become a factual must for suppliers once a Step 3-decision has been taken, which makes the use of a cloud service supplier of a certain level of assurance compulsory for a given economic activity. Without such a Step 3-decision there is no obligation as to the use of a cloud service and hence certification should remain optional.

538 https://eucoc.cloud/en/detail/news/press-release-ready-for-submission-eu-cloud-code-of-conduct-finalized/

539 With the switching and porting working group (SWIPO) a stakeholder working group is currently designing such code of conduct.

540 Recitals 30-31, Art. 6 Regulation (EU) 2018/1807

541 Art. 56 (2), Regulation (EU) 2019/881

542 Art. 56 (3), Regulation (EU) 2019/881

543 Art. 56 (4–6), Art. 58, Art. 60 Regulation (EU) 2019/881

2.3.2.3 *Step 3: Regulatory requirements for cloud use by selected economic activities*

In a third step, the use of cloud services by economic actors in certain sectors can be made conditional upon the use of a cloud provider of a certain assurance level of the cloud security certification schemes outlined above. Any such requirement must be the result of a case-by-case inquiry by a competent authority affirming that risks are unlikely to be sufficiently internalised by actors in the sector concerned for reasons related to a public good, lack of competition or prohibitively high costs.

2.3.2.3.1 Standards for regulatory requirements

It is essential that all **regulatory requirements** meet the following standards:

- **They must be risk-based and fact-driven:** Any regulatory requirement concerning the use of cloud services must be the result of an objective risk assessment including the probability and consequence of an adverse event. If the requirement is justified by the lack of competition on the regulated identity's market, this must be substantiated.
- **They must be proportionate:** Regulatory requirements concerning the use of cloud services limit entrepreneurial freedom and may cause costs which must be proportionate to the expected benefit of the regulated cloud use..
- **They must not distort competition between cloud service providers:** Any regulatory requirement as to the assurance level of a cloud service must be neutral as to the identity of the cloud service provider actually used by the regulated entity. Any cloud service provider should be able to apply for certification regarding all levels of assurance. The regulated entity should be free in picking a cloud provider of the required assurance level and in negotiating the terms of use.
- **They must not distort competition between regulated entities:** As regulatory requirements may cause costs to regulated entities and these entities may compete with others, an unequal application of regulatory requirements may distort competition. Ideally, within an economic sector, similar risks should be treated with similar regulatory requirements.

Avoiding an unlevel playing field between regulated entities presupposes (1) harmonised cloud security certification schemes (see above in Step 1) and (2) a harmonised application of regulatory requirements to entities in a given sector. Whereas the CSPCERT WG recommends – at least partly – ENISA to issue guidelines as to which certification and assurance level is deemed appropriate for which use cases[544], we recommend a more binding approach as to avoid the said unlevel playing field. In the following we will differentiate between three sub-steps in Step 3 in order to reach an application of regulatory requirements, which is as uniform as possible within sectors.

544 The CSPCERT WG also provides for some possible examples. For instance, personal web page hosting, connected lights or video streaming could require a 'basic' assurance level. Heating settings, telecommunications or payment services supported by cloud services could fall under the 'substantial' category. A 'high' assurance level may be appropriate for management services on critical infrastructure, medical records, core financial services deployed by a cloud service provider, or eIDAS identity services in the cloud. [p. 24 and 25]

2.3.2.3.2 Step 3a: A consistent identification of essential service operators

The Directive on the security of network and information systems across the Union[545] ("NIS Directive") is the first horizontal European legislation concerning cybersecurity. Amongst others, the directive requests Member States to "ensure that operators of essential services take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations".[546]

The Directive lists seven sectors (energy, transport, banking, financial market infrastructure, health sector, drinking water supply and distribution and digital infrastructure) and a number subsectors which are seen as essential.[547] Member states were required to identify by November 2018 all "operators of essential facilities with an establishment on their territory". The directive lists some criteria for Member States to apply when doing so.[548] A "cooperation group", consisting of national experts and representatives from the Commission and ENISA shall "support Member States in taking a consistent approach in the process of identification of operators of essential services".[549]

Although the NIS-Directive does give quite some guidance regarding (sub)sectors of essential services, it remains uncertain whether Member States will apply the directive's criteria as to identify essential operators in a consistent way. Apart from the "cooperation group", the directive entails no governance mechanism to guarantee such consistent identification of essential service operators. In fact, the Commission has recently found "a considerable degree of fragmentation across the Union when it comes to the identification of operators of essential services".[550]

The Directive is rather cautious is setting out how the level of consistency of the identification process amongst Member States can be improved. Information provided by Member States to the Commission and the list of service operators established by each Member State "would serve as further input in the assessment of the regulatory practice of each Member State with a view to ensuring the overall level of consistency of the identification process amongst Member States".[551]

An inconsistent identification has two drawbacks. First, there is a security risk as not all essential facility operators in the EU may be identified as such and may consequently not be subject to the directive security requirements. Given the high degree of economic interlinkage between EU Member States, the costs of any such risk materialising would not be limited to the Member State directly affected. Secondly, competition between economic actors will be distorted when the activity of an operator is found to be essential in one Member State, but not so in another Member State. The costs of additional security requirements would put the former at a competitive disadvantage. This argument is valid in particular for four of the seven identified sectors in which cross-border activity is especially relevant (energy, transport, banking, financial market infrastructure)

Given the cross-border implications in the internal market, we recommend an additional governance mechanism to guarantee a consistent identification of essential service providors by all Member

545 Directive (EU) 2016/1148 of 6 July 2016
546 Article 14 (1) Directive (EU) 2016/1148
547 Annex II Directive (EU) 2016/1148
548 Article 5 (1) and (2) Directive (EU) 2016/1148
549 Article 5 (6) Directive (EU) 2016/1148
550 EU-Commission (2019c), The Commission criticises a „variety of methodologies", „diverging interpretations" and „significant inconsistencies" which „could have a negative impact on achieving the Directive's goals".
551 Recital 23 Directive (EU) 2016/1148

States. We recommend focussing on energy, transport and financial market infrastructure as they show a particularly high potential for distorting competition. Banking is subject to a sophisticated set of sector-specific rules, which already cover cloud use as an element of outsourcing (see below). For this reason, the sector-specific rules will apply.[552] Given supervisory structures in the EU banking industry, the added value of an additional governance mechanism for this industry is limited.

We recommend a more formal role of the "cooperation group" for the energy and transport sector as well as for financial market infrastructure (but not for banks). For each of these three sectors, one (or more) working group shall be installed. The members of each working group shall consist of the ENISA as well as the respective national competent authority (for that sector). If existent, sector-specific supervisors shall also be members of the working group. In that case, the national and European supervisor will both be a member. Each working group of the cooperation group shall vote with a simple majority upon the identification of essential service operators in all Member States.

2.3.2.3.3 Step 3b: Agreement on the application of the EU cloud security certification scheme

Once essential service operators have been consistently identified across the EU, it is necessary to safeguard that, upon requesting appropriate security requirements regarding the use cloud services, all competent authorities apply the EU cloud security certification scheme.

If (and only if) national competent authorities (according to the NIS-Directive) and sector-specific supervisors (relevant are especially financial supervisors) impose security requirements regarding the use of cloud services by an essential service operator or a supervised entity, they shall demand the use of a cloud service provider of a specified assurance level, using the EU cloud security certification scheme.

Given the high level of discretion of both national competent authorities and sector-specific supervisors, there is no need for an additional legal basis for this agreement.

2.3.2.3.4 Step 3c: A uniform application of the EU cloud security certification scheme within sectors

After agreeing upon EU cloud security certification scheme standards (Step 1), installing a system of voluntary certification (Step 2), identifying operators of essential services in a consistent way across the EU (Step 3a) and agreeing on applying the EU cloud security certification scheme under NIS-action and when performing sector specific supervision regarding cloud services (Step 3b), it is important to safeguard that similar cloud security issues within a sector are treated in a similar way. For comparable risk related to comparable activities within a sector, authorities in all Member States should request the use of cloud services on an identical level of assurance. If this were not the case, competition in the internal market would be distorted as some operators of essential services would face higher costs than others.

As the regulatory and supervisory framework of relevant industries greatly varies, there is no standard answer as to how a uniform application of the EU cloud security certification scheme can be guaranteed. In the following we differentiate between three groups of sectors.

552 Recital 9 Directive (EU) 2016/148

Group 1: Banking, financial market infrastructure, insurance and securities. In finance, the use of cloud services by financial undertakings is already covered by sector specific regulation as it is seen as "outsourcing", which is covered by a number of acts of secondary legislation in the financial field.[553] The level of regulation of outsourcing (and hence cloud use) already depends upon operational functions or activities being "critical or important".[554] This approach fits well to different levels of assurance set out in the cloud certification scheme.

In its FinTech action plan, the EU-Commission suggested the EU financial supervisory authorities (ESAs) propose guidelines for outsourcing to cloud service providers by the first Quarter of 2019.[555] The European Banking Authority (EBA) has already issued such guidelines[556], which are addressed to banks as well as to competent authorities (i.e. national banking supervisors and the ECB, which directly supervises all significant banks in the Eurozone). EIOPA (for insurance) and ESMA (for securities) will publish guidelines soon and have announced a close alignment with the EBA.[557,558]

- Given the EBA's cloud guidelines, the challenge in the banking sector is to guarantee a uniform application of those guidelines to different economic activities in the banking sector. This is not trivial, as the guidelines themselves do not (and most likely will not in the future) allocate an economic activity to a cloud assurance level. They rather set abstract rules regarding governance and risk management related to outsourcing certain tasks.
- As a consequence, banking supervisors will be decisive actors in reaching a uniform application of the EU cloud security certification scheme. Financial supervision is characterised by a significant degree of discretion by the supervisory authority. This is necessary to allow the supervisor to swiftly and appropriately react to different risks at hand. In principle, this level of discretion makes the supervisor very apt to guarantee a uniform application of cloud security certification schemes to different banking activities.
- At least for all large ("significant") banks of the Eurozone, the European Central Bank, in its capacity as single supervisor of those banks, is able to guarantee such uniform application without any legislative change being necessary. In this way, a significant share of the EU's banking sector would be subject to a uniform application of the EU cloud certification scheme.
- The case is different for all non-Eurozone-Banks and for the bulk of smaller banks within the Eurozone, which are all supervised by national authorities. Exceptional measures and soft-power-like competencies may allow the ECB and the EBA to exert pressure on national supervisors to follow a uniform approach.[559]

---

553 Directive 2014/65/EU (Markets in Financial Instruments Directive; MiFID II) contains provisions regarding the outsourcing in investment services and activities. Directive 2015/2366/EU (Payment Service Directive; PSD2) sets out requirements for outsourcing by payment institutions. Directive 2009/138/EC (Solvency II) address operation risks and governance when outsourcing.

554 For Insurance: Article 49 Directive 2009/138/EC and Article 274 Solvency II Delegated Regulation (EU) 2015/35; for securities: Article 16 (5) Directive 2014/65/EU and Article 39 MiFID II Delegated Regulation (EU) 2017/565; for payments: Article 19 Directive 2015/2366/EU.

555 COM(2018) 109

556 EBA (2019)

557 EIOPA (2019)

558 Id, page 5.

559 The ECB may take on at any time the direct supervision of less-significant banks, which are normally supervised by national authorities (Art. 6 para. 5. (b) Council Regulation (EU) No. 1024/2013). The EBA may issues non-binding guidelines adressing national authorities (Art. 16 Regulation (EU) No 1093/2010) and settle disagreements between national authorities (Art. 19 Regulation (EU) No 1093/2010).

In insurance and securities, there is no European supervisory authority with powers similar to those of the ECB in Eurozone banking. EIOPA and ESMA function – like the EBA – in a federal-like models without being in the position to guarantee a uniform application of cloud security certification schemes to different activities in the field of securities and insurance. Similar to the EBA, they may exert soft pressure on national supervisors.

All in all, at least in the current supervisory set-up, the ECB's supervisory powers may enable a uniform application of the EU cloud security certification amongst the Eurozone's biggest banks. This will avoid distortions of competition between those banks. For smaller banks, insurances and security firms, it remains to be seen, whether the ESA's soft powers will suffice to reach such an outcome. We recommend to evaluate the situation by the End of 2020. In the absence of a uniform application, level 2-action may be considered. In that case, the relevant secondary legal acts (MiFID II, Solvency II) may be complemented with a empowerment for the Commission to adopt delegated acts which allocate insurance and security activities to a level of cloud assurance. The EIOPA and ESMA would be tasked with offering technical advice in the form of regulatory technical of implementing technical standards. These delegated acts are binding in nature and are likely to allow a uniform application of cloud security certification schemes to different financial activities, also in the absence of direct decision powers for European supervisory authorities.

Group 2: Energy and transport. Despite a great body of European sector-specific regulation in these areas, the management of risks related to cloud computing has not been the focus of said regulation. Any cloud-related measures are hence likely to emanate from the application of the NIS-Directive. Also, in these sectors, the degree of European supervision is less intensive as compared to the finance industry. ACER, the EU-Agency for the Cooperation of Energy Regulators primarily has a coordination function between national authorities with very few direct decision powers.

As cross-border competition in these sectors is particularly intense, it is important to reach a uniform application of the EU cloud security certification with respect to all operators.

We suggest the establishment for each subsector (e.g. air transport) of a new decision-making body which shall be responsible for safeguarding a uniform application. The body shall consist of representatives of the sectoral supervisors, both from the national and European level as well as representatives of the cybersecurity authorities, both national and ENISA. Depending on the number of cases to be decided, a decision-making system may be installed where decision by national authorities regarding the application of the EU cloud security certification scheme are valid, unless a set number of member of the body oppose to that decision.

Group 3: Health, water and digital infrastructure. Markets for products and services in these markets tend to be national or even local, mainly given physical restriction due to immovable infrastructure (water and digital infrastructure). For this reason, cross-border competition in these sectors is of limited relevance.

Following the subsidiarity principle, we suggest measures regarding the application of the EU cloud security certification scheme in the sectors of health, water and digital infrastructure to be taken by

national authorities and to abstain from a fully harmonised approach.

2.3.2.3.5 The role of the public sector

For the public sector as well, ENISA may establish different levels of assurance of cloud services, using the cloud security certification scheme (Step 1). Different levels of assurance may fit to different cloud activities of the public sector, depending i.a. on the necessary level of security and confidentiality.

A mandatory certification is hence unnecessary (Step 2). Given the potential of the public sector as a cloud customer, cloud service providers will have a self-interest in being certified along the standards set out for the public sector if the latter endorses the standard. If the public sector does not endorse the standard, there is no use in making certification mandatory.

It is unlikely that Member States will be willing to accept Steps 3a and 3c, i.e. a coordination of decisions allocating public sector activities to certain levels of assurance by cloud providers. Such matters touch the core of national sovereignty and it may be too sensitive for administrations and governments to give up discretion. From an economic point of view, this must not pose a problem as it does not result in distortions of competition or impediments in the internal market.

It is of utmost importance for the public sector to agree on Step 3b, i.e. to agree in principle on the application of the EU cloud security certification scheme. Even though administrations may allocate their activities to cloud assurance levels in a non-uniform manner, such endorsement by the public sector would increase the relevance of the EU cloud security certification scheme and the providers adhering to it.

2.3.3 Summary of Recommendation No. 17

Recommendation No. 17

We propose an EU Framework for secure and trusted cloud computing that addresses concerns related to data security, data governance and service availability in the cloud. The growing use of cloud services brings about a lot of economic advantages, but at the same time confronts us with political and operational risks which may endanger the continuous availability of services which are essential to our economies. The public good character of cloud service availability justifies public intervention.

We propose the creation of an EU Framework for Secure and Trusted Cloud Computing as a model of public intervention regarding the use of cloud services which is proportionate, efficient and non-discriminatory. It consists of three steps.

In Step 1, the EU should define common requirements for secure and trusted cloud computing that will address user concerns related to data security, data governance and service availability. As requested by the European Commission, the ENISA should draft baseline cloud computing security certification schemes regarding general use. In addition, ENISA should draft complementary cloud computing security certification schemes for public administrations and sectors providing essential services (according to the NIS-Directive).

In **Step 2**, the existing modalities for the issuing of certificates in the Cybersecurity Act can be applied to the certification of cloud service suppliers without any change. There is no need for making certification compulsory.

In **Step 3**, the use of cloud services by economic actors in certain sectors can be made conditional upon the use of a cloud provider of a certain assurance level of the cloud security certification

schemes. Any such regulatory requirements must be risk-based, proportionate and may not distort competition, neither between cloud service providers nor between regulated entities.

In order to reach a uniform application of these regulatory requirements, we recommend in **Step 3a** a consistent identification of essential service operators to whom regulatory requirements will apply. For this reason, we propose a more formal role for the NIS-Directive's "cooperation group" to identify operators from the energy, transport and financial market sector (but not for banks).

After confirming in **Step 3b** that cloud security requirements for essential service operators will follow the EU cloud security certification scheme, it is necessary in **Step 3c** to safeguard a uniform application of the certification scheme. In the financial industry, the well-developed supervisory structure may be sufficient to reach this aim. For the energy and transport sector, we suggest the establishment of new decision-making bodies of sectoral supervisors and cybersecurity authorities which shall be responsible for safeguarding a uniform application. Given the national nature of markets for health, water and digital infrastructure, we suggest national authorities should be responsible for the application of the cloud certification schemes.

Although a uniform application of the EU cloud security certification scheme in the public sector is unlikely, the national use by the public sector of the certification scheme would increase the relevance of the EU cloud security certification scheme and the providers adhering to it.

2.3.4 GAIA-X and the blueprint

2.3.4.1 What is GAIA-X?

In October 2019, the German federal ministry for economic affairs and energy announced the "GAIA-X" project at the German Digital Summit in Dortmund.[560] It was presented as a project to establish a "high-performance, competitive, secure and trustworthy data infrastructure for Europe".[561] GAIA-X is a federated decentral data infrastructure that combines cloud as well as edge computing[562] instances from different providers.[563] A pool of companies[564], associations[565] and academic actors[566] participate in the project. Although it has been perceived mainly as a German project, it is by design open and actively seeking for further collaboration with stakeholders of other EU Member States and "open to market participants outside Europe who share our goals of data sovereignty and data availability".[567]

GAIA-X pursues to following goals[568]:

- strengthen Europe's digital sovereignty by gaining back a level playing field and ensuring full control by the user of a data infrastructure over saved and processed data,

560 Bundesministerium für Wirtschaft und Energie (2019)
561 Id. p. 2
562 Edge computing means that data processing does not necessarily occur in the cloud but closer to where it is generated (i.e. near to where production takes place). Edge computing is used mostly for real-time applications, where time constraints matter [Id. p. 6].
563 Id. p 3.
564 Collaborating companies are e.g. the Robert Bosch GmbH, Bundesdruckerei GmbH, DE-CIX Management GmbH, Atos SE, Deutsche Telekom AG, SAP SE and Festo AG & Co. KG.
565 Collaborating associations are e.g. Bitkom e.V., VDMA e.V. and Bundesverband der Deutschen Industrie e.V.
566 Collaborating actors from science are e.g. Fraunhofer Institute for Software and Systems Engineering and Berlin Institute of Health and Charité – University Medicine Berlin.
567 Bundesministerium für Wirtschaft und Energie (2019)
568 Id. p. 3–12.

- support B2B data-sharing by allowing independent decisions on who may access data under which terms and conditions,
- lower the dependency of users of cloud solutions on products and services delivered by third-country providers, in particular from the hyperscalers in the US and China,
- increase the scalability of European cloud providers by enabling users to resort to multiple cloud or edge instances and, thus, enhance the competitiveness of European cloud providers,
- lower the dependency of users of cloud solutions on products and services delivered by third-country providers, in particular from the hyperscalers in the US and China,
- increase the scalability of European cloud providers by enabling users to resort to multiple cloud or edge instances and, thus, enhance the competitiveness of European cloud providers,
- strengthen the visibility and transparency of European cloud providers,
- help companies in the data economy to innovate,
- prevent existing lock-in problems and allow for better interoperability between providers and services and
- create incentives, especially for small and medium sized companies (SMEs), to take the plunge from on-premise to more efficient cloud solutions by increasing trust, preventing dependencies and lowering investment costs.

2.3.4.2 Features

The GAIA-X project has several features: The connected decentral data infrastructure consists of different so-called GAIA-X-Nodes set up as public, private or edge cloud. Providers must offer a self-description of the characteristics of each node they deliver to the network. Such description will include information on where data is stored and processed, on levels of data sovereignty based on certifications, on pricing and other technical, legal or content criteria. The data infrastructure shall incorporate only secure and open technologies. Interfaces shall ensure that the exchange of data within the network occurs simply and secure. Common standards shall make data integration and migration easy. Components for the network shall be made available by a software and service repository. Services required for each node and for the exchange between nodes like identification and authorisation services should be provided homogeneously and are implemented as functions ('Function as a Service') to allow for interoperability and avoid lock-in scenarios. Service providers that wish to participate in GAIA-X must comply with common standards and undergo a certification process by independent third parties, which includes "IT security, service levels, the degree of data sovereignty attained, and contractual framework conditions" (see Figure 22).[569]

[569] Bundesministerium für Wirtschaft und Energie (2019), p. 12 and 13

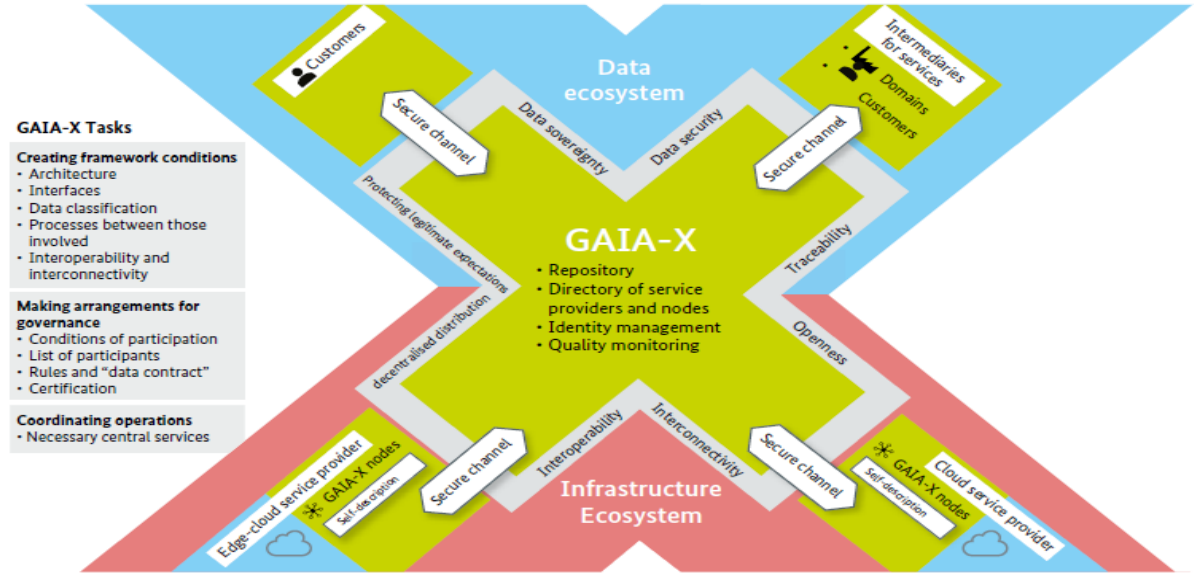

Figure 22: The GAIA-X data infrastructure and ecosystem
Source: Bundesministerium für Wirtschaft und Energie (2019)

In order to set-up the GAIA-X data infrastructure network, the project collaborators propose to create a central organisation that would define the reference architecture, set common standards, provide for criteria for a certification framework and decide upon the certification of applying providers.[570]

2.3.4.3 Compatibility of GAIA-X with the blueprint

According to Step 2 of the blueprint, Gaia-X providers may request a certification of their services according to the certification scheme. The services will be allocated to the relevant level of assurance.

If in Step 3c, authorities request the use of cloud services by an economic actor of a certain level of assurance, Gaia-X will be available as a potential supplier if it has been certified into this assurance level of the cloud computing security certification schemes. The same goes for all other cloud service suppliers in this assurance level as certification is available to all providers meeting the relevant requirements.

Given its objective and setup, GAIA-X is expected to meet requirements for data governance and service availability. However, non-EU cloud providers may well attempt to adapt the architecture of their physical and legal infrastructure in order to meet those requirements. If they meet the criteria, they should be allowed to serve the market as to enable a fair competition between all cloud providers.

570 Id. p. 3.

Bibliography

Accenture (2017), Why AI is the future of growth by Marc Purdy and Paul Daugherty, Online at: www.accenture.com/t20170524t055435__w__/ca-en/_acnmedia/pdf-52/accenture-why-ai-is-the-future-of-growth.pdf

AGCOM (2018), Big data Interim report in the context of the joint inquiry on "Big data" launched by the AGCOM deliberation No. 217/17 / CONS, Department of Economics and Statistics

Akerlof, G.A. (1978), The market for "lemons: Quality uncertainty and the market mechanism, Academic Press

Arrow, K.J. (1972), Economic welfare and the allocation of resources for invention, Readings in industrial economics. Palgrave, London

Article 29 Working Party (2017), Guidelines on Consent under the General Data Protection Regulation (GDPR), WP 259

Article 29 Working Party (2017), Opinion on the definition of consent, WP187

Bates, B.J. (1990), Information as an economic good: A re-evaluation of theoretical approaches, in B. D. Ruben and L. A. Lievrouw (eds.), Mediation, Information, and Communication

Bauer M., Ferracane M., Lee-Makiyama H. and van der Marel E. (2016), Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localisation Measures in the EU Member States, ECIPE Policy Brief No. 03/2016.

Berinato S. (2015), There's No Such Thing as Anonymous Data, Harvard Business Review, February 09, 2015.

Bonneau V. and Mahieu B. (2013), Analysis of cloud best practices and pilots for the public sector, Study for the European Commission, SMART 2012/0069

Böttcher (2011), „Clearstream" – Die Fortschreibung der Essential Facilities-Doktrin im Europäischen Wettbewerbsrecht, Beiträge zum Transnationalen Wirtschaftsrecht, Heft 102

Bundesministerium für Wirtschaft und Energie (2019), Das Projekt GAIA-X: Eine vernetzte Dateninfrastruktur als Wiege eines vitalen, europäischen Ökosystems, https://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/das-projekt-gaia-x.pdf?__blob=publicationFile&v=18

Bundesministerium für Wirtschaft und Energie (2019a), Ein neuer Wettbewerbsrahmen für die Digitalwirtschaft - Bericht der Kommission Wettbewerbsrecht 4.0

Bundesministerium für Wirtschaft und Energie (BMWi) (2019b), Die volkswirtschaftliche Bedeutung von digitalen B2B-Plattformen im Verarbeitenden Gewerbe, September 2019

Burri, M. (2019), Understanding the Implications of Big Data and Big Data Analytics for Competition Law, New Developments in Competition Law and Economics. Springer, Cham

Christakis T. (2019), 21 Thoughts and Questions about the UK/US CLOUD Act Agreement, European Law Blog, October 2019

Cisco (2018), White paper, Global Cloud Index: Forecast and Methodology, 2016–2021

Crémer J., de Montjoye Y. and Schweizer H. (2019), Competition policy for the digital era, Final Report for DG Competition of the EU Commission

Deloitte (2017), Study on emerging issues of data ownership, interoperability, (re-)usability and access to data, and liability, Deloitte, Study prepared for the EU Commission, SMART 2016/0030

Deloitte et al. (2018), Study to support the review of Directive 2003/98/EC on the re-use of public sector information, Final Report, European Commission, SMART 2017/0061

Demary V., Guggenberger N., Rabovskaja E. and Rusche C. (2019), Data Sharing im E-Commerce, Rechtliche und ökonomische Grundlagen, Institut der Deutschen Wirtschaft

Dewenter, R. and Rösch J. and Terschüren A. (2014), Abgrenzung zweiseitiger Märkte am Beispiel von Suchmaschinen, Working Paper Series No. 151, Helmut Schmidt Universität

Dewenter, R., Lüth, H. (2018), Datenhandel und Plattformen, Assessing big data, Study prepared for the German Federal Ministry of Education and Research

Drexl (2017), Designing Competitive Markets for Industrial Data – Between Propertisation and Access 8 (2017) JIPITEC 257

Drexl et al. (2016), Ausschließlichkeits-und Zugangsrechte an Daten, Positionspapier des Max-Planck-Instituts für Innovation und Wettbewerb, 16 (2016): 914-918.

Duch-Brown, N., Martens B. and Mueller-Langer F. (2017), The economics of ownership, access and trade in digital data, JRC Digital Economy Working Paper 2017-01

EBA (2019), EBA Guidelines on outsourcing arrangements, EBA/GL/2019/02

EIOPA (2019), Outsourcing to the Cloud: EIOPA's Contribution to the European Commission Fintech Action Plan, doi:10.2854/774288

EU-Commission (2004), Commission Notice on informal guidance relating to novel questions concerning Articles 81 and 82 of the EC Treaty that arise in individual cases (guidance letters), OJ C 101/78, 27.4.2004

EU-Commission (2009), Communication from the Commission — Guidance on the Commission's enforcement priorities in applying Article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings, in: Official Journal of the European Union OJ C 45, 24.2.2009, p. 7–20

EU-Commission (2009a), Report on the functioning of Regulation 1/2003, Communication from the Commission to the European Parliament and the Council COM (2009) 206 final

EU-Commission (2009b), Staff working paper accompanying the Communication from the Commission to the Council Report on the functioning of Regulation No 1/2003, SEC(2009) 0574 final

EU-Commission (2012), Antitrust Manual of Procedures, Internal DG Competition working documents of procedures for the application of Articles 101 and 102 TFEU, March 2012, doi 10.2763/78829, available at http://ec.europa.eu/competition/antitrust/antitrust_manproc_3_2012_en.pdf

EU-Commission (2016), An emerging offer of "personal information management services" - Current state of service offers and challenges, Brussels

EU-Commission (2017), Communication by the EU-Commission, Building a European Data Economy, COM (2017) 9

EU-Commission (2018), International Digital Economy and Society Index 2018

EU-Commission (2018a), Communication 'Towards a Common European Data Space', COM(2018) 232 final

EU-Commission (2019), Communication from the Commission to the European Parliament and the Council, Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union, COM/2019/250

EU-Commission (2019a), DG Trade Statistical Guide, July 2019, DOI 10.2781/258389

EU-Commission (2019b), Recommendation for a Council Decision authorising the opening of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters, COM(2019) 70

EU-Commission (2019c), Report assessing the consistency of the approaches taken by Member States in the identification of operators of essential services in accordance with Article 23(1) of Directive 2016/1148/EU on security of network and information systems, COM(2019) 546

EU-Commission (2019d), Rethinking Strategic Autonomy in the Digital Age, EPSC Strategic Notes Issue

EU-Commission (2019e), Annex: all reports of the workshops on "common European data spaces", July to November 2019, available at: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63832

European Data Protection Supervisor (2017), Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content

European Data Protection Supervisor (2020), Preliminary Opinion on Data Protection and scientific Research, January 2020

European Supervisory Authorities (2018), Joint Report: Regulatory sandboxes and innovation hubs, JC 2018 74, 2018

European Union Agency for Fundamental Rights and Council of Europe (2018), Handbook on European data protection law - 2018 edition

Evans D. (2009): Two sided-markets, available at: www.oecd.org/daf/competition/44445730.pdf.

Everis (2018), Study on data sharing between companies in Europe, Study prepared for the EU Commission, SMART 2016/0087

FedRAMP (2011), PolicyMemo, Memorandum for chief information officers

FedRAMP (2017), Security Assessment Framework, Version 2.4

Filistrucchi L. (2008), A SSNIP Test for Two-sided Markets: The Case of Media, Working Paper #08-34, Tilburg University & University of Siena, October 2008

Fröhlich-Bleuler, G. (2017), Eigentum an Daten, Jusletter of 6 (2017).

Gabel D., Hickman T. (2019), Data Protection Authorities – Unlocking the EU General Data Protection Regulation, White & Case Publications, 5 April 2019, accessible at

https://www.whitecase.com/publications/article/chapter-14-data-protection-authorities-unlocking-eu-general-data-protection

German Federal Ministry of Economic Affairs and Energy and French Ministry for the Economy and Finance (2019), A Franco-German Manifesto for a European industrial policy fit for the 21stCentury

González Fuster G., Scherrer A. (2015), *Big Data and Smart Devices and Their Impact on Privacy. Study for the LIBE Committee*, European Parliament, Directorate-General for Internal Policies, Policy Department C Citizens' rights and constitutional affairs

Goodridge, P. R., Chebli O. and Haskel J. (2015), Measuring activity in big data: New estimates of big data employment in the UK market sector, Working Papers 25158, Imperial College, London, Imperial College Business School.

Graef, I. (2015), Market definition and market power in data, in: The case of online platforms, World Competition 38.4 (2015)

Graef, I. (2016), Data as essential facility, Competition and innovation on online platforms, Wolters Kluwer

Graef I., Wahyuningtyas Y. and Valcke P. (2015), Telecommunications Policy 2015, Vol. 39, No. 5, p. 375-387

Hoffmann A. and Eckhardt P. (2017), Free Flow of non-personal data (Regulation), cepPolicyBrief No. 33/2017

Immenga and Mestmäcker (2012), Wettbewerbsrecht Band 1: EU/Teil 1, Kommentar zum Europäischen Kartellrecht, 5. Auflage 2012, C.H. Beck Verlag, München

International Data Corporation (IDC) and Open Evidence (2017), European Data Market, Study prepared for the EU-Commission, SMART 2013/0063 Final Report

International Data Corporation (IDC) and the Lisbon Council (2019), Second Report on Facts and Figures: Updating the European Data Market Study Monitoring Tool, Update of the European Data Market Study, Study prepared for the EU-Commission, SMART 2016/0063

International Monetary Fund (2019), World Economic Outlook Database

IWConsult (2019), Readiness Data Economy, Bereitschaft der deutschen Unternehmen für die Teilhabe an der Datenwirtschaft

Jones, C. and Tonetti C. (2018), Nonrivalry and the Economics of Data, 2018 Meeting Papers. Vol. 477. Society for Economic Dynamics

Kathuria, V. and Globocnik, J. (2019), Exclusionary Conduct in data-driven markets: Limitations of data sharing remedy, Max Planck Institute for Innovation and Competition Research Paper No. 19-04

Kerber, W. (2016), A new (intellectual) property right for non-personal data? An economic analysis, Gewerblicher Rechtsschutz und Urheberrecht, Internationaler Teil (GRUR Int) 11 (2016): 989-999.

Knieps, G. (2008), Wettbewerbsökonomie: Regulierungstheorie, Industrieökonomie, Wettbewerbspolitik, Springer

Koenig, C. and Schreiber, K. (2010), Europäisches Wettbewerbsrecht, Tübingen

Körber, T. (2004), Recht der Internationalen Wirtschaft (RIW) 2004

Körber (2007), Microsoft-Urteil des EuG, WuW 12/2007, p. 1209 (1217).

Korff D. and Georges M. (2019), The DPO Handbook Guidance for data protection officers in the public and quasi-public sectors on how to ensure compliance with the European Union General Data Protection Regulation, Fondazione Basso Ricerche Progetti

Koutroumpis, P., Leiponen A., and Thomas L. (2017), The (unfulfilled) potential of data marketplaces, ETLA Working Papers No. 53

Krippendorff, K. (1985), Information, information society and some marxian propositions, Informatologia Yugoslavica 17.1-2 (1985)

Krotova, Rusche and Spiekermann (2019), Die ökonomische Bewertung von Daten: Verfahren, Beispiele und Anwendungen. IW-Analysen No. 129

Laitenberger J. (2018), *EU competition law: relevance anchored in empiricism*, CRA Conference, Brussels

Langhanke C. and Schmidt-Kessel M. (2015), Consumer Data as Consideration, (2015) 4 Journal of European Consumer and Market Law, Issue 6

Legatum Institute (2019), Global Index of Economic Openness: A report published by the Legatum Institute in partnership with Templeton World Charity Foundation

Linde, F. (2009), Ökonomische Besonderheiten von Informationsgütern, Wissens- und Informationsmanagement, Gabler Verlag

Mańko R. and Monteleone S. (2017), Contracts for the supply of digital content and personal data protection, Briefing of the European Parliamentary Research Service, Brussels

Martens, B. (2018), The impact of data access regimes on artificial intelligence and machine learning, Joint Research Centre Working Paper No. 2018-09

McKinsey Global Institute (2017), China's Digital Economy, A leading global force, Discussion Paper

McKinsey Global Institute (2019), Innovation in Europe, Changing the game to regain a competitive edge, McKinsey Global Institute, Discussion paper, October 2019

McNutt, P. (1999), Public goods and club goods, Encyclopedia of law and economics 1 (1999): 927-951

Meisel, L. and Spiekermann, M. (2019), Datenmarktplätze – Plattformen für Datenaustausch und Datenmonetarisierung in der Data Economy, Fraunhofer Institut für Software und Systemtechnik, ISST-Bericht

Mell P. and Grance T. (2011), "The NIST definition of Cloud computing," NIST Special Publication

Mestmäcker and Schweitzer (2014), Europäisches Wettbewerbsrecht, 3. Auflage, C.H. Beck

Monopolkommission (2014), Wettbewerbspolitik: Herausforderung digitale Märkte, Sondergutachten 68

Mulligan S.P. (2018), Cross-Border Data Sharing Under the CLOUD Act, Congressional Research Service Report, R45173

Netherlands Ministry of Economic Affairs and Climate Policy (2019), Dutch Digitalisation Strategy, Dutch vision on data sharing between businesses, February 2019

OECD (2011): OECD Technical workshop on the economics of regulation, available at: www.oecd.org/tad/services-trade/48964759.pdf

OECD (2015), Data-driven innovation: Big data for growth and well-being, OECD, Paris.

OECD (2017), *OECD Science, Technology and Industry Scoreboard 2017: The digital transformation*, OECD Publishing, Paris, https://doi.org/10.1787/9789264268821-en.

OECD (2017a), Safe Harbours and Legal Presumptions in Competition Law – Background Note by the Secretariat, DAF/COMP(2017)9

OECD (2018), "Private Equity Investment in Artificial Intelligence", OECD Going Digital Policy Note, OECD, Paris, www.oecd.org/going-digital/ai/private-equity-investment-in-artificial-intelligence.pdf

OECD (2019), Licensing of IP rights and competition law – Note by the EU, DAF/COMP/WD(2019)52

Panzar, J.C., Willig, R.D. (1977), Free Entry and the Sustainability of Natural Monopoly, Bell Journal of Economics, 1977, vol. 8, issue 1, 1-22

Poikola A., Kuikkaniemi K. and Honko H. (2018), A Nordic Model for human-centered personal data management and processing, White Paper of the Ministry of Transport and Communications of Finland

PWC (2017), Global artificial intelligence Study, available at: https://www.pwc.com/gx/en/issues/analytics/assets/pwc-ai-analysis-sizing-the-prize-report.pdf

Reinsel et al. (2018), The Digitization of the Word, IDC White Paper, Nov 2018

Ricardo, D. (1891), Principles of political economy and taxation. G. Bell

Ritter C. (2018), *Presumptions in EU Competition Law*, 6 J. Antitrust Enforcement 189

Roland Berger and Internet Economy Foundation (IEF) (2019), Wettbewerb für die Cloud – Wie Unternehmen und Verwaltung von Multicloud-Lösungen profitieren

Rusche, C. and Scheufen M. (2018), On (intellectual) property and other legal frameworks in the digital economy: An economic analysis of the law, IW-Report No. 48/2018

Pindyck S. and Rubinfeld L. (2005), Mikroökonomie, 6. Auflage, 2005, Pearson Studium

Schweitzer, H. and Peitz M. (2017), Datenmärkte in der digitalisierten Wirtschaft: Funktionsdefizite und Regelungsbedarf?, ZEW Discussion Papers No. 17-043

Shapiro C. and Varian H. (1998), Information rules: a strategic guide to the network economy. Harvard Business Press

Stigler, G.J., (1968), Barriers to Entry, Economics of Scale and Firm Size, in: George J. Stigler, The Organization.

The Joint Institute for Innovation Policy (JIIP) et al. (2019), Study on mapping Internet of Things innovation clusters in Europe, Study prepared for the EU-Commission, SMART 2015/0012

Thieulin, B. (2019), Towards a European digital sovereignty policy, Opinion of the Economic, Social and Environmental Council (ESEC), March 2019

Timan, T. and Mann Z., (eds) (2019), Data protection in the era of artificial intelligence. Trends, existing solutions and recommendations for privacy-preserving technologies, October 2019, BDVA

U.S. Department of Justice (2019), Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, White Paper, April 2019

UNCTAD (2019), Digital Economy Report 2019, Value creation and capture: Implications for developing countries

Van Gorp and Batura (2015), Challenges for competition policy in a digitalised economy, Study for the ECON Committee of the European Parliament, July 2015, p. 52.

Van Roosebeke B. (2008), Gutachten zur Überarbeitung des EU-Rechtsrahmens für elektronische Kommunikation, Centrum für Europäische Politik (cep)

Vestager M. (2016), Big Data and Competition, Speech delivered at the EDPS-BEUC Conference on Big Data, Brussels, 29 September 2016

Vomfell, L. et al. (2015), A classification framework for data marketplaces. No. 23. Working Papers, ERCIS-European Research Center for Information Systems

Wendehorst C. (2017), Of Elephants in the Room and Paper Tigers: How to Reconcile Data Protection and the Data Economy, in Lohsse S., Schulze R., Staudenmayer D. (eds.), Münster Colloquia on EU Law and the Digital Economy –Trading Data in the Digital Economy: Legal Concepts and Tools, 2017

Whish R. and Bailey D. (2018), Competition Law, Ninth Edition, Oxford University Press

Willems, H. (2017), Trading in Data: An Industry Perspective, Trading Data in the Digital Economy: Legal Concepts and Tools. Nomos Verlagsgesellschaft mbH & Co. KG

Wils W. (2013), *Ten Years of Regulation 1/2003-A Retrospective*, Journal of European Competition Law & Practice, Volume 4, Issue 4, August 2013, pp. 293–301

Woods A.K. (2016), *Against Data Exceptionalism*, 68 STAN.L.REV.

Woods A.K. (2018), Litigating Data Sovereignty, Yale Law Journal, Vol. 128

Wylie B., McDonald S. (2018), What Is a Data Trust?, Center for International Governance Innovation

Zins, C. (2007), Conceptual approaches for defining data, information, and knowledge, Journal of the American society for information science and technology 58.4: 479-493.

Authors:

Dr. Bert Van Roosebeke heads the cep Department for Information Technology.

Dr. Martina Anzini, Philipp Eckhardt and Anne-Carine Pierrat are policy analysts at the cep Department for Information Technology.

cep | Centre for European Policy

Kaiser-Joseph-Strasse 266 | D-79098 Freiburg

Phone +49 761 38693-0 | www.cep.eu

cep is the European policy think tank of the non-profit organisation Stiftung Ordnungspolitik. It is an independent centre of excellence specialising in the examination, analysis and evaluation of EU policy. The offices of cep are located in Freiburg, Berlin and Paris.