EUROPEAN
COMMISSION

Brussels, 23.2.2022
SWD(2022) 34 final

COMMISSION STAFF WORKING DOCUMENT

IMPACT ASSESSMENT REPORT

Accompanying the document

Proposal for a Regulation of the European Parliament and of the Council

on harmonised rules on fair access to and use of data
(Data Act)

{COM(2022) 68 final} - {SEC(2022) 81 final} - {SWD(2022) 35 final}

Table of Contents

1. INTRODUCTION: ECONOMIC, POLITICAL AND LEGAL CONTEXT

This Impact Assessment accompanies the legislative proposal for a Data Act. The initiative aims to address issues that slow down the development of the data economy across sectors in Europe. These issues have been consistently flagged by stakeholders, Member States, members of the European Parliament and experts as unresolved.

This initiative is a key pillar of the European Strategy for Data[1], which aims to create a single market for data where data flows between sectors and Member States, where ample data is available for use, and where data is used in line with European rules and values.

The Data Act complements the two other major instruments shaping the European single market for data. While the Data Governance Act[2] focuses on trusted mechanisms for data **sharing** and the Digital Markets Act[3] on fair **competition** between gatekeepers and other market players, also in relation to the use of data, the Data Act would enable wider data **use** across the economy, notably by regulating the fundamental questions of who can use the data generated by connected products and related services, and what are the conditions for such use.

The Data Act would apply to data understood as any digital representation of acts, facts or information and any compilation of such acts, facts, or information, including in the form of sound, visual or audiovisual recording. This wide definition ensures consistency with the Data Governance Act[4] and builds on a time-tested approach in the field of open data where a similar definition has been in force since 2003[5].

These three areas of focus (share, compete, use) have been fully embraced by the co-legislators. The interinstitutional negotiations on the Data Governance Act (data sharing) were finalised on 30 November 2021, only a year after the Commission made its proposal. For the Digital Markets Act (compete), both co-legislators are finalising their position. They indicated the need to go further on **usage** issues in the context of the Data Act proposal.

The Data Act would cover the following areas:

- Use of data in an Internet-of-Things context: rules on who can use which data generated by connected products and related services are essential for competitive aftermarkets, for ensuring consumer choice and for promoting innovation as we move into an era in which everything is connected. The cross-sectoral rules would also frame the conditions for future data access rights established in sector-specific legislation.

[1] COM(2020) 66 final.
[2] COM(2020) 767 final.
[3] COM(2020) 842 final.
[4] COM(2020) 767 final, see Article 2(1).
[5] OJ L 172, 26.6.2019, p. 56–83, see Article 2(6).

- Data contracts: while freedom of contract would remain the underlying rule, the Data Act would address manifestly abusive or excessive conditions related to data use in contracts.
- Use of data in business-to-government contexts ('B2G'): unlocking the value of data from private companies in exceptional situations where current data access mechanisms by the public sector are inefficient, for example in cases of public emergency.
- Improving the performance of the essential enablers for data exchange: data processing services and data standards.

1.1. Economic and societal context

According to the International Data Corporation, the data economy was estimated to be worth over EUR 324.86 billion at the end of 2019[6], representing 2.6% of the GDP of the EU-27. The data economy has a substantial growth potential. However, as noted in President von der Leyen's 2020 State of the Union address, while *'[a] real data economy […] would be a powerful engine for innovation and new jobs […] the reality is that 80% of industrial data is still collected and never used.'*

Data is the basis for many new digital products and services, in particular for developing artificial intelligence (AI) applications. The expansion of the Internet-of–Things (IoT) technologies and devices creates new data sources. A recent study predicts that by 2030, the services and products linked to the IoT could enable $5.5 trillion to $12.6 trillion in value globally[7]. A growth in value generation from data will lead to a larger sustainable growth and innovation dividend on the wider economy[8]. Research by the Organization for Economic Cooperation and Development (OECD) suggests that companies that invest in data-driven innovation and data analytics exhibit faster productivity growth than those that do not by approximately 5% to 10%[9]. Data is a critical resource for start-ups and SMEs, in particular, as a business can be set up with very low initial capital[10]. Some 85% of new jobs in the data economy over the last years have been created by SMEs[11].

In response to the COVID-19 crisis, the Communication on the recovery plan[12] stresses that Europe *'must build a real data economy as a motor for innovation and job creation'* and calls for a Data Act to establish the conditions for better access to and control of industrial data at large.

Data is also critical to achieving the Green Deal objectives, such as supporting the circular economy, reducing waste as well as adapting to and combating climate change.

[6] European Commission (2020). *Final Study Report of the Updated European Data Market Study*.
[7] McKinsey (2021). *Internet of Things: Catching up to an accelerating opportunity.*
[8] European Commission (2020). *The Updated European data market study*.
[9] OECD (2015). *Data-driven innovation: big data for growth and well-being*, Paris.
[10] European Commission (2020). *Final Study Report of the Updated European Data Market Study*.
[11] European Commission (2021). *Small companies create 85% of new jobs*, Press Release.
[12] COM(2020) 456 final.

Furthermore, studies estimate that a better use of data could save EUR 120 billion per year in the EU health sector alone[13], while insights from disaster loss data could have mitigated the enormous human and financial losses caused by extreme weather in Europe[14]. In the transport, buildings and industry sectors, real-time analytics of data generated by physical energy networks leads to average savings of 10-20%[15].

1.2. Political context

The socioeconomic potential of data has been addressed through a range of legislative and policy measures in the EU in recent years. In the 2018 Communication 'Towards a common European data space', the Commission issued a series of principles to guide business-to-business (B2B) and B2G data sharing[16]. It committed to monitor progress and, if necessary, consider legislative intervention to tackle any persistent problem.

Echoing the European strategy for data of February 2020, the European Council Conclusions of 21 October 2021 stressed the importance of making rapid progress on existing and future initiatives in the digital policy domain, in particular '*unlocking the value of data in Europe, notably through a comprehensive regulatory framework that is conducive to innovation and facilitates better data portability, fair access to data and ensures interoperability*'[17]. The EU Data Strategy clearly indicates that these issues should be tackled by the Data Act.

The European Parliament in its resolution on the European strategy for data urged the Commission to present a Data Act to encourage and enable a greater and fair access to and use of data in B2B, B2G, government-to-business (G2B) and government-to-government (G2G) situations, in all sectors[18].

1.3. Legal context

EU legislation has until now focused on removing barriers to the free flow of data across the internal market, safeguarding fundamental rights of individuals with regard to personal data protection, increasing trust in data sharing and enhancing the supply of public and private sector data for innovative reuse. The table below provides an overview of which problems are and are not solved by existing instruments.

Main issues in the data economy	**Status** ✓ -solved ✗ - not solved
Lack of free flow and insufficient protection of personal data	✓GDPR

[13] European Commission (2020). *Shaping the digital transformation in Europe*, by McKinsey, p. 26.
[14] Extreme weather events are calculated to have caused 307 547 fatalities between 1970 and 2019, and average losses of EUR 12 billion per year; SWD(2020) 330 final/2; European Environment Agency, *Economic losses from climate-related extremes in Europe - Indicator Assessment*; World Meteorological Society (2021). *Water-related hazards dominate disasters in the past years*, Press Release.
[15] IEA (2019), *Energy efficiency and digitalisation*, IEA, Paris; Askenazi, B. (2019). *IA et Big Data révolutionnent l'efficacité énergétique*, Les Échos.
[16] COM(2018) 232 final; SWD(2018) 125 final.
[17] European Council meeting conclusions of 21 and 22 October 2021.
[18] European Parliament resolution of 25 March 2021 on a European strategy for data (2020/2217(INI)).

Lack of free flow of non-personal data/data localization requirements	✓FFoD Regulation
Lack of trust in data intermediaries	✓Data Governance Act (DGA) proposal
Insufficient availability of public sector data for re-use	✓ Open Data Directive and DGA for sensitive public data
Imbalances caused by the market power of gatekeepers	✓Digital Markets Act proposal
Owners of connected products do not get value out of their data	✗
Contractual imbalance between data holders and data users in data access and use that cannot be solved by competition law	✗
Insufficient means to access private sector data by public sector bodies in exceptional situations	✗
Lack of interoperability between cloud services and hurdles to effective switching between providers across the market (beyond gatekeepers)	✗
Lack of data interoperability	✓ Governance structures (DGA – Data Innovation Board) ✗ Intervention capacity

The **Free Flow of Non-Personal Data Regulation (FFoD)**[19] ensures that non-personal data can be stored, processed and transferred anywhere in the EU. The Data Act would make it easier for businesses and citizens to exercise this right in practice. The FFoD Regulation also addresses the problem of 'vendor lock-in' at the level of providers of data processing services, by introducing self-regulatory codes of conduct to facilitate switching data between cloud services. As the self-regulatory approach seems not to have affected market dynamics significantly, the Data Act presents a regulatory approach to the problem highlighted in the Free Flow of Non-Personal Data Regulation.

With regards to personal data, a general access and portability right exists under the **General Data Protection Regulation** (GDPR). Under Article 20 GDPR, the data subject has the right to receive their personal data held by a controller and transmit it to another controller, or to have the data transmitted – where technically feasible – directly from one controller to another. This might include data generated by connected products and related services. However, the exercise of this right has proven largely theoretical, and it does not entitle the data subject to continuous or real-time access to the data, which is essential for products that are always connected to the internet. Furthermore, differences in interpretation by industry and supervisory authorities on what types of data should be in scope impede its meaningful application in practice. Indeed, empirical evidence, notably in the recent preliminary report of the Commission's sector inquiry into consumer IoT products, indicates that this right is rarely exercised. Moreover, no equivalent provision exists for non-personal data, and portability between cloud providers is largely out of scope.

[19] OJ L 303, 28.11.2018, p. 59–68.

Another important relation is that between the Data Act and the **Digital Markets Act** ('DMA'), for example with regard to portability obligations for cloud service providers. The DMA presents a direct portability obligation vis-à-vis targeted problematic services of gatekeepers, in line with the special responsibility of such providers on the market. However, additional intervention would be necessary because vendor lock-in issues reach further than gatekeepers. This is particularly visible in the 'platform as a service' (PaaS) and 'software as a service' (SaaS) cloud markets, where interoperability problems are gravest and where hyperscalers have a smaller share of the market. Therefore, the Data Act would present a complementary set of minimum framework conditions to enable switching, which would apply horizontally across the market and preserve the asymmetric approach of the DMA versus gatekeepers.

Beyond tackling the issues related to the fairness of cloud and edge services, the Data Act would enhance this portability right for data generated through the use of connected products, excluded from the scope of the DMA. The Data Act would, in particular, not extend other obligations foreseen for gatekeepers under the DMA, thus keeping a clear distance between the two legal regimes. Finally, the policy objective of the DMA, which is to limit the ability of gatekeepers to combine and exploit data from large numbers of data holders to undermine contestability and fairness in core platform services will be reflected in the Data Act by ensuring that the increased data supply primarily benefits users and smaller economic players.

Interplay Data Act - DMA on cloud switching (more detailed table in Annex 5)

	Data Act	Digital Markets Act
Covered entities	Horizontal market Coverage	Targeted coverage
Type of intervention	Symmetric: Framework conditions + interoperability standardisation	Asymmetric: Direct obligation + enforcement
Scope	Cloud/edge switching (includes switching of data, applications, and services)	Portability of data (will apply mostly to simple data storage services operated by gatekeepers)

The objective of the **Digital Services Act**[20] (DSA) is to modernise the rules laid down by the eCommerce Directive 2000/31 by improving the mechanisms for the removal of illegal content and for the effective protection of users' fundamental rights online. It will create a stronger oversight of online platforms and intermediaries, including obligation to disclose to regulators information related to algorithms used or on targeted advertising.

The Data Act would not directly interfere with the subject matter of the DSA in B2B situations, as it focuses on regulating data access in the Internet of Things relationships rather than in the online services environment. However, both acts share a common goal

[20] COM/2020/825 final

of rebalancing the digital economy in favour of smaller economic players and of empowering the users of digital services. In this context, the main objective of the Data Act is to ensure that the largest online service providers targeted by both the DMA and the DSA do not become the main beneficiaries of the newly created rights on data access and portability.

In the area of B2G data access, Article 31 of the DSA creates a procedure for the European Commission and national authorities to access data held by platforms for monitoring, enforcement and research purposes. Despite similarities with the planned provisions of the Data Act that would also allow for privately held data to be used by researchers, both the objective and the scope of the provisions in these two instruments are quite different. While the DSA aims to further research into "systemic risks" to fundamental rights to privacy or freedom of expression, the Data Act would allow for conducting research on data obtained from the private sector only within the limits of the purpose for which the data was requested (e.g. to address a public emergency or to fulfil other, strictly defined exceptional data needs).

The impact of the **Database Directive** is also significant - it provides for the *sui generis* protection of databases created through a substantial investment, even if the database itself is not an original intellectual creation protected by copyright. Even though there has been substantial case-law interpreting the provisions of this Directive, the Data Act proposal addresses ongoing legal uncertainties about whether databases containing data generated by products and services would be entitled to such protection. .Annex 6 to this Impact Assessment looks at the review of this directive, focusing on the problematic expansion of the protection of the *sui generis* right to machine-generated data.

Regarding competition rules, the 2019 report prepared for Vice-President Vestager on 'Competition policy in the digital era' indicates that competition law cannot solve all the issues in the data economy. The problems tackled in the Data Act, such as those in the case of data generated by connected products and related services or cloud interoperability, are systemic rather than a result of the dominance of specific market players. In the case of connected products and related services, no single player is a dominant player on the primary market for most products (market for the sale of cars, connected agri-tech machinery, household appliances, medical devices).

Furthermore, as regards data-sharing contracts, almost all will be below the threshold of a dominant market position. The issue here is the risk of an abusive use of an imbalance between contractual parties, not of the market structure. The imbalance originates from the fact that the party requesting the data, who needs it to develop or run innovative digital business models, can only get the data from the data holder. The latter retains 'de facto' exclusivity over the data collected by the device.

Similar considerations guide the need to set horizontal rules on data pricing: without them, unreasonable prices could be set by data holders, rendering access impossible in practice. This issue cannot be solved by relying on the notion of the abuse of a dominant

position given the thresholds for dominance and the length and complexity of competition procedures.

As regards the relation between the Data Act and sectoral legislation (see also Annex 5), rights could either be established product by product, or through a coherent horizontal approach complemented by sectoral specifications where necessary. Both from the political debate and the interaction with stakeholders it results that the latter approach is preferable. A patchwork of sector-specific rules would be inefficient. At the same time the Data Act should avoid over-regulating by setting very detailed requirements that apply in all the sectors in the dynamically evolving technological landscape. It would therefore follow the approach already applied and tested in the context of the NIS (security of network and information systems) Directive, consisting of a common horizontal framework on which sector-specific legislation can build.

The Data Act would set common basic rules for all sectors, most of which are unregulated as regards rights to use data, such as in the areas of smart machinery and consumer goods. Likewise, the Act would not change existing legislation (in sectors such as automotive[21], energy[22] and banking[23]), however future legislation should in principle be aligned with the horizontal principles of the Data Act. Finally, the Act should leave room for vertical legislation to set more detailed rules addressing sector-specific technical aspects of data access, for example cyber-security, data formats or covering issues going beyond data access as such. For example, the high technological maturity of the automotive sector might justify complementing the Data Act with rules on access to vehicle functions (e.g. to run vehicle diagnostic routines or remote door unlocking) and to vehicle resources, such as a dashboard/infotainment system (i.e. to communicate with the driver).

Annex 5 presents the relationships summarised above in more detail. Annex 11, paragraph 4 presents the interplay between the contractual unfairness test and a proposal for DMA, competition law in general and the proposal for a DSA.

1. PROBLEM DEFINITION

2.1. What are the problems?

In line with the European strategy for data[24], the overall problem tackled by this initiative is the insufficient availability of data for use and reuse in the European economy or for societal purposes. In contrast to traditional economic resources, many parties can use the same dataset for various purposes without functional loss to the original data collector. However, this potential of data as a non-rival economic good is not being fully realised. Legal, economic and technical issues related to data use affect a range of sectors, as evidenced by a survey of 14 EU industrial ecosystems performed by the Commission[25]

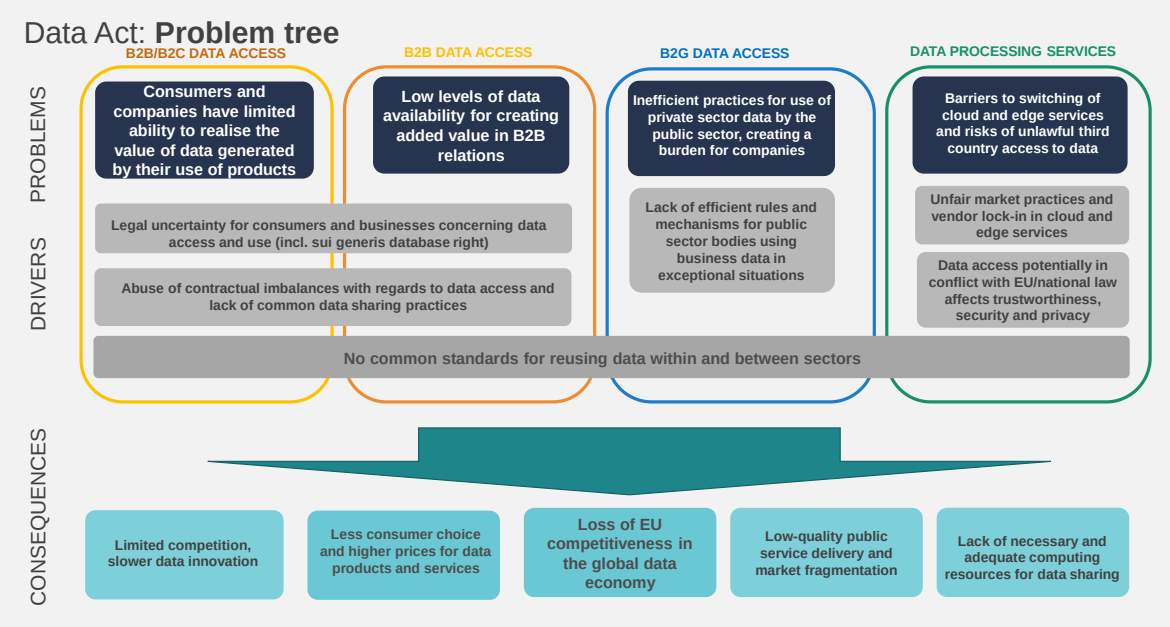
[21] OJ L 151, 14.6.2018, p. 1–218.
[22] OJ L 158, 14.6.2019, p. 125–199.
[23] OJ L 337, 23.12.2015, p. 35–127.
[24] See Chapter 4 and COM(2020) 66 final.
[25] European Commission (2022). *Industrial ecosystems survey - Main findings*, Report.

and as validated by the public consultation on the Data Act. Further details and concrete examples of those problems are provided in Annex 7.

According to a report on the economic potential of non-personal industrial data, only 43% to 58% along a value chain and 20% to 40% of such potential between sectors is realised[26]. This is confirmed by other studies which indicate that, apart from a handful (8%) of companies, businesses are not capturing value from data, with only small gains in a few isolated experimental use cases[27]. Furthermore, in the consultation on the Data Strategy, 75% of responding businesses confirmed they had difficulties in accessing the data they need from other companies[28]. Stakeholder feedback also shows that the non-binding B2B and B2G data-sharing principles issued in 2018 have not been effective, because problems persist[29]. Stakeholders, especially SMEs, considered the principles not helpful enough to improve their ability to access data in practice[30]. The report by an expert group on B2G data sharing[31] confirmed these doubts. The Commission survey on EU industrial ecosystems detected the persistence of serious obstacles to data availability and use[32]. Furthermore, the support study to this impact assessment clearly indicates that barriers to data access and use in B2B and B2G contexts persist[33].

The next sections will consider the problems driving this underutilisation of data in detail. Due consideration must also be given to the fact that while regulatory intervention on the access to and use of data opens opportunities, it could also lead to certain risks, such as cybersecurity risks, competition/ competitiveness issues, potential misappropriation of the data, and data protection breaches. Annex 8 provides an overview of these risks and how they are relevant in the context of the Data Act.

[26] Deloitte (2018). *Realising the economic potential of machine-generated, non-personal data in the EU*, Report for Vodafone Group, p. 30.
[27] Bisson P. *et al.* (2018). *Breaking away: The secrets to scaling analytics*, McKinsey.
[28] European Commission (2020). *Outcome of the online consultation on the European strategy for data*.
[29] COM(2018) 232 final; SWD(2018) 125 final.
[30] European Commission (2019). *SME panel consultation B2B data sharing - Final Report*.
[31] European Commission (2020). *Towards a European strategy on business-to-government data sharing for the public interest*, Final Report of the High-Level Expert Group on B2G Data Sharing.
[32] European Commission (2022). *Industrial ecosystems survey - Main findings*, Report; European Commission High-Level Expert Group on B2G *website*.
[33] European Commission (2022). *Study to support an Impact Assessment on enhancing the use of data in Europe*. Study prepared by Deloitte.



Problem 1 – Consumers and companies have limited ability to realise the value of data generated by their use of products and related services

Since the adoption of the 'Building a European Data Economy' Communication in 2017[34], the stakeholders from all sectors have consistently flagged the problems related to data generated from connected products as requiring EU level action. Accordingly, the EU Data Strategy indicated the 'issues related to usage rights for co-generated data (such as IoT data in industrial settings)' as a priority area for possible legislative intervention[35]. The use of connected products (such as smart home appliances or fitness trackers) increasingly generates data. A '**connected product**' in this context means a tangible item able to communicate data via a publicly available electronic communications service, whose primary function is not the storing and processing of data. It generates, by means of its physical components, data concerning its performance, use or environment. Sometimes these connected products are accompanied by services (e.g. lifestyle advice) that use the generated data as input. Such '**related service**' means a digital service which is incorporated in, or inter-connected with, a product and is essential for the product to perform its primary function. However, the buyers of those products only have a limited possibility to benefit from the value of the data generated by using them, since they lack effective control over the data. This raises the issue of what users can expect in terms of who can use the data when they buy such products.

While the problem is very relevant for consumers, commercial users of connected products and related services (especially SMEs) face the same obstacles. The issue of who can benefit from the value of the data equally applies to B2C and B2B situations. In the agri-food, construction or manufacturing sectors, owners of smart machinery report being unable to access valuable data generated through their use of those products, and

[34] COM(2017) 9 final.
[35] COM/2020/66 final.

that the data is captured by platform intermediaries or the equipment manufacturers[36]. Ensuring frictionless data access and use is critical to boosting the European machine-to-machine economy[37].

	Example of a connected product	Example of a problem due to the inability to realise the value of data or to access/use data generated by one's own connected product
B2B	• Braking system of a tractor • Lifts • Factory machine	Manufacturer denies the data access request, making maintenance (especially predictive) and repair services provided by an independent service provider impossible, or inhibiting innovation based on data.
B2C	• Smart dishwasher • Cleaning robot • Fitness tracker • Smart solar panels	Manufacturer denies the data access request by a third-party who might provide a digital solution (e.g. more efficient energy use) to the owner of the object based on a combination of data from different connected products.

The use of certain products generates large volumes of data but, for personal data, the obligation on data controllers to transfer data to a third-party service provider (Article 20 GDPR) is limited: it does not apply to non-personal data, the scope is restricted to certain data (on the basis of consent or contract) and unclear as to e.g. observed data.

In certain areas (electricity, banking, cars), sectoral legislation ensures that selected third parties can have access to the relevant data if the consumer so requires. However, the issue of lack of control of consumers over the data they generate is transversal, and the underlying questions are common to all sectors, namely: in practice, can consumers choose who can reuse the data they generate? Who benefits from the generated value?

More transparency on what data is being created and is accessible, better control over their data and the possibility to give selected third parties access to the data would benefit consumers and companies using connected products and related services. They could choose alternative aftermarket services, which depend on access to such data[38], or make better-informed decisions when buying more sustainable products and services[39].

Consumers and companies using connected products and related services would be able to repair products at competitive prices, thereby extending their lifespan. A major German stakeholder association predicts that, as a result of more individualised repair and servicing, consumers could pay up to 40% less for such services[40]. Ultimately, better control over data would lead to a broader use of the data for economic or other purposes and would increase the overall benefits of data for the economy.

[36] Van der Burg, S., Wiseman, L. and Krkeljas, J. (2020). *Trust in farm data sharing: reflections on the EU code of conduct for agricultural data sharing*, Ethics Inf Technol.
[37] COM(2020) 66 final; Special Advisor's Report.
[38] MEASURE (2021). *The Measure privacy report*.
[39] SWD(2019) 92 final.
[40] Position paper submitted by Zentralverband Deutsches Handwerk in the context of the public online consultation on the Data Act, see *here*.

Problem 2 – Low levels of data availability for creating added value in B2B relations

Today, digitalisation efforts in every sector depend on the availability and use of data. In certain situations, beyond the use of connected products, data access is a precondition for market entry, participation in a supply chain or innovation. This applies for example, to situations where new and innovative applications depend on the analysis of data amassed and held by other business entities. However, the data is often not made available at all or only under commercially prohibitive terms, such as excessive pricing, which especially affects SMEs.

A start-up needs citizens' mobility data to develop a sustainable and smart mobility app for a big city. The start-up cannot develop this app without mobility data from a widely spread mobility service provider active in that city. That service provider exploits this situation and imposes excessive contract terms on data access and use on the start-up. The start-up is left with no other choice than to accept these terms or refrain from developing its innovative business model.

While sectoral legislation and some codes of conduct exist[41], the bulk of data access and use of data by companies relies on contracts. It is therefore significant that 65% of companies replying to the online consultation experienced problems when trying to get access to data with other companies by way of contracts[42]. The most prominent reasons given by these respondents in this context were outright refusal of granting access not linked to competition concerns (55%), abuse of contractual imbalance (44%) and unreasonable prices (42%)[43]. A similar message emerged from the ecosystem analysis carried out by the Commission services[44]. Companies regularly face strict contractual limitations e.g. when seeking to use data needed to provide products and services such as installing machinery and repair[45].

In the following situations the contractual issues around data are particularly pertinent, especially from the perspective of SMEs. First, these issues impact the relations between companies that buy an object or a service that generates data and the manufacturer or service provider. Second, they concern situations where the data use is part of a contract in the context of a supply chain. Finally, they concern data sharing contracts between businesses (see example in the box above).

The obstacles to data access and use prevent the materialization of substantial economic and societal benefits. Companies confirmed, in response to the online consultation on this initiative, that increasing the use of data would lead to extra performance, development of new services and business models, better supply chains, anticipating problems in the

[41] E.g. EU Code of conduct on agricultural data sharing by contractual agreement.
[42] European Commission (2022). *Outcome of the online consultation on the Data Act*.
[43] European Commission (2022). *Outcome of the online consultation on the Data Act*.
[32] European Commission (2022). *Industrial ecosystem survey – Main findings*, Report.
[45] European Commission (2018). *Study on emerging issues of data ownership, interoperability, (re-)usability and access to data, and liability*, prepared by Deloitte.

production line, reducing carbon footprint and increased cooperation between innovators[46].

According to the OECD, data access and reuse could generate social and economic benefits worth between 1% and 2.5% of GDP[47]. One study found that increasing the level of data reuse among companies could create as much as EUR 1.3 trillion a year in the manufacturing sector by 2027 by improving productivity[48]. Another study estimated the costs of not addressing the problem of insufficient and inefficient B2B data reuse, based solely on the notion of estimated foregone profits of data suppliers, which would amount to EUR 185 billion in the period 2021-2030[49] - a number that would be even higher for data users as their need for data is higher.

Problem 3 – Inefficient practices for use of private sector data by the public sector, creating a burden for companies

Data is essential for driving better delivery of policy and public services. Increasingly, the data used in evidence-based policymaking is created outside of the public sector and held by a minority of very large companies. Public sector bodies typically acquire such data from the private sector by setting reporting obligations, launching public procurement, or encouraging voluntary data-sharing collaborations. However, these mechanisms show clear limitations, such as being too slow.

This concerns in the first place emergency situations. The COVID-19 crisis has confirmed the difficulties in the timely acquisition of data necessary for crisis management by governments at national, regional, and local levels[50] as well as by European institutions.

The COVID-19 crisis showed the importance of public authorities having access to aggregated and anonymised location data coming from mobile network operators as well as social network service providers. The data is essential for analysing the effect of mobility on the spread of the virus, including informing early warning systems for potential new outbreaks and taking the right measures to combat the crisis. However, practice showed that there were no established processes in place for obtaining such data.

However, there may be other situations where data use by the public sector can yield substantial benefits, without unduly burdening the private sector. This is for example the case where new ways of collecting the data ensure are more efficient and could in the

[46] European Commission (2022). *Outcome of the online consultation on the Data Act*.
[47] OECD (2019). *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies*, OECD Publishing, Paris.
[48] Deloitte (2018). *Realising the economic potential of machine-generated, non-personal data in the EU*, Report for Vodafone Group, p. 9.
[49] European Commission (2022, *forthcoming*). *Study on model contract terms and fairness control in data sharing and in cloud contracts and on data access rights*, study prepared by ICF (section 2.2.3.2).
[50] De Nigris, S. *et al.* (2020). *Artificial Intelligence and digital transformation: early lessons from the COVID-19 crisis*; several EU and international case studies available in a Data & Policy special collection dedicated to *Telco Big Data Analytics for COVID-19*, see *here*; Science Academies of the Group of Seven (G7) (2021). *Statement on Data for international health emergencies: governance, operations and skills*.

future replace reporting obligations (e.g. replacing questionnaires from statistical offices by the use of aggregated scanner data from supermarkets).

The difficulties in obtaining the data in these *ad hoc* situations were also highlighted by a High-Level Expert Group, which concluded that data held by private sector was of enormous potential value for improving public service deliver, but that data reuse in B2G contexts in Europe was hampered by an increasingly fragmented landscape of operational models and rules between and within Member States and sectors, lack of structures and incentives for businesses, while the processes for the reuse of businesses' data by public sector bodies were not transparent, scalable or easily replicable[51]. Indeed, public sector bodies identify legal barriers and legal uncertainty due to different rules in Member States as the main factors impeding reuse of private sector data (88% and 80% respectively), together with the lack of appropriate infrastructures and costs (82%)[52].

Therefore, the unavailability of data in situations where the need for data could not have been easily foreseen in advance and where the use of the data is a necessary condition for the public sector body to fulfil its statutory tasks is primarily a problem for the public sector. At the same time, companies face multiple unclear and uncoordinated requests for data from different public sector bodies[53], putting an undue administrative burden on them. Also, companies operating in different Member States potentially have to comply with different sets of national rules and practices. The support study has found indications of a growing trend to issue such requests and of a corresponding rise in the administrative burden and compliance costs. As the data availability gaps are not likely to be addressed to a sufficient degree by legislative means (e.g. by new reporting requirements), the problem of unavailability of data for public use objectives is also of relevance for the private sector, albeit indirectly – as a source of unnecessary additional costs.

Furthermore, obstacles to cross-border cooperation persist. *'B2G data sharing lacks a framework that would provide transparency and harmonisation across Member States'*, stated a business association stakeholder in a recent consultation[54]. Given the increasing cross-border nature of many challenges public authorities have to face, such as extreme weather events, health emergencies, environmental degradation, the lack of access to relevant data hampers the effectiveness of their actions.

Problem 4 – Barriers to switching of cloud and edge services and risks of unlawful third country access to data

Data are useless without data-processing infrastructures. Different types of data-processing services, notably cloud and edge computing services, provide the

[51] European Commission (2020). *Towards a European strategy on business-to-government data sharing for the public interest*, Final Report of the High-Level Expert Group on B2G Data Sharing.
[52] European Commission (2022). *Outcome of the online consultation on the Data Act*.
[53] European Commission (2022). *Study to support an Impact Assessment on enhancing the use of data in Europe*. Study prepared by Deloitte.
[54] Feedback from ACT- The app association, see European Commission *webpage*: *Have your Say - Data Act & amended rules on the legal protection of databases.*

technological basis that makes data access and use possible. Not having a competitive market for cloud and edge services in place is an additional obstacle in the value creation on the basis of data for many actors. Therefore, access to competitive cloud and edge services needs to be ensured for stakeholders in the data economy[55].

This objective is currently obstructed by user concerns around the fairness and trustworthiness of cloud and edge services and the confidentiality and integrity of data, which lead to lower levels of adoption.[56] The academic literature specifically pinpoints two issues as the two most important determining factors in this respect, with security ranking first, and vendor lock-in (specifically in PaaS and SaaS contexts) second[57].

The *fairness* of cloud and edge services is at stake where users are inhibited to switch from one provider to another because of contractual, economic, and technical obstacles. An important part of this widely acknowledged problem[58] is a lack of interoperability, particularly with regard to PaaS and SaaS services offered by a myriad of providers (often SMEs). This does not only result in lower cloud adoption but is also problematic for data access and use, given that users are simply locked into a single service and therefore unable to freely adopt the cloud and edge services that offer the innovative data-sharing functionalities that they need.

Furthermore, widespread concerns of *trustworthiness* of cloud and edge services and *confidentiality and integrity* of data are being voiced, regarding particularly the unlawful access by non-EU/EEA governments to data stored in the cloud[59]. This was confirmed in the last stakeholder consultation, in which only 0.7% of respondents indicated not to see unlawful access to their data by non-EU/EEA governments as a risk[60]. The problem is relevant because at present, 85% of the cloud services provided in Europe are offered by providers headquartered outside the EU/ EEA[61]. This leads to two issues: firstly, the confidentiality, security and integrity of data is potentially affected by unlawful access; and secondly, a macro-economic risk associated to security of supply of cloud services, which is increasingly problematic as European businesses are becoming more and more

[55] Snowflake (2021). *The pitfalls of ETL processing*, see *here*.
[56] J. Scholten (2016). *The determinants of cloud computing adoption in The Netherlands: a TOE-perspective*, see *here*; J. Opara Martins, R. Sahandi and F. Tian (2016). *Critical analysis of vendor lock-in and its impact on cloud computing migration: a business perspective*, see *here*; N. Loutas et al. (2013). *Cloud computing interoperability: the state of play*, see *here*; D. Petku and A. Vasilakos (2014). *Portability in clouds: approaches and research opportunities*, see *here.*
[57] European Commission (2018). *Switching of cloud services providers*, prepared by International Data Corporation (IDC) and Arthur's Legal, p. 88.
[58] European Commission (2018). *Switching of cloud services providers*, prepared by International Data Corporation (IDC) and Arthur's Legal; IT Daily/BELTUG (2020). *Security policies and vendor lock-in top priority for Belgian companies*, see *here*; EPRS (2016). *Cloud computing: an overview of economic and policy issues*, see *here.*
[59] Y. Lechelle (2021). *It is time to strengthen our EU data sovereignty - Open Letter to EU institutions*, see *here*; EDPB/EDPS (2019). *Initial legal assessment of the impact of the US CLOUD Act on the EU legal framework for the protection of personal data and the negotiations of an EU-US Agreement on cross-border access to electronic evidence*, see *here;* CEPS (2015). *Access to electronic data by third country law enforcement authorities – Challenges to the rule of law and fundamental rights*, see *here*.
[60] European Commission (2022). *Outcome of the online consultation on the Data Act*.
[61] Synergy research group (2021), and *here*, figures pertain to IaaS/PaaS and private cloud services.

dependent on cloud services[62]. In 2020, among enterprises that used cloud computing services, 59% were 'highly dependent', while 38% were dependent to an 'upper-medium' extent[63].

2.2. What are the problem drivers?

Driver 1 – Legal uncertainty for consumers and companies concerning data access and use

Companies consider the complexity of legislation governing who can do what with data on which conditions as a significant obstacle to a more efficient use of data[64]. In situations where the data is generated by machines through the use of products and related services by businesses and consumers, it is unclear whether the acquisition of an object includes the benefit of having a share in the value of the data. Businesses reported also legal uncertainties as to the measures available to counter the risks of loss of control and misappropriation of data by data recipients or third parties, which are risks described in more detail in Annex 8.

One source of uncertainty is the question of the applicability of the Database Directive to machine-generated data.

Role of the Database Directive in data access and use

The sui generis *database right set out in the Database Directive is an intellectual property right that grants an exclusive right to the makers of databases. However, with the rapid development of the data economy where vast amounts of data are automatically generated through all economic activities, it becomes difficult to clearly distinguish which databases should be protected by the* sui generis *right and which not. This is due to the fact that IoT technologies produce vast volumes of data in order to carry out their functions efficiently. This data may be stored in databases, which are necessary for the operation of the IoT tools (e.g. optimising temperature in a house, directing a car fleet or increasing crop production in arable land). However, these databases are only a by-product of the activity carried out by the equipment manufacturer or by the user of the connected object.*

As a result of the current uncertainty as to whether the sui generis *right may apply to databases containing machine-generated data, there is an increasing risk that the* sui generis *right would be used opportunistically for purposes that exceed the intended goal of IP protection of databases. The second evaluation of the Database Directive has already documented this risk, which is well understood by a significant proportion of stakeholders[65].*

In the 2017 study supporting the Evaluation of the Database Directive, a clear majority of respondents was against the sui generis *right's expansion to machine-generated data[66]. The results of the survey conducted for the current review show that respondents consider it necessary to clarify the scope of the* sui generis *right. 74% maintain that excluding machine-*

[62] Centrum für Europäische Politik (2020), *European leadership in the digital economy*, see *here.*
[63] Ibid.
[64] SITRA (2021). *The future of the European companies in the data economy*, Report.
[65] SWD(2018) 146 final.
[66] European Commission (2018). *Study in support of the evaluation of Directive 96/9/EC on the legal protection of databases*, prepared for DG CNECT by JIIP and Technopolis Group.

generated data will have positive effects on obtaining legal certainty and the majority sees positive effects for innovation and research activities[67]*. The need to review the* sui generis right *in relation to the status of machine-generated data is also supported by the majority (54%) of stakeholders in the online consultation conducted in 2021 for the Data Act. The review of the 1996 Database Directive (examined in detail in Annex 6) complements the Data Act because it prevents the* sui generis *protection from being expanded to machine-generated data, as this would present an obstacle to the sharing and use of data.*

The legal uncertainties also pertain to the portability and interoperability of data. Limited control is given to data subjects, i.e. natural persons, by the GDPR. An individual has rights regarding personal data generated by their use of a product, including the right to access those data, as laid out in applicable data protection rules. They also have the right to port data (Article 20 GDPR) in a structured, commonly used, and machine-readable format. The exercise of the right to data portability is, however, limited to only personal data processed for the performance of a contract or based on consent. It excludes notably data processing on the basis of legitimate interests (Article 6(1)(f) GDPR) and does not apply to non-personal data. Data protection authorities and industry disagree on whether data about the data subject which is observed but not consciously provided by the data subject should be in scope of Art 20. It has also practical limitations: it is not designed to enable real-time data use in digital ecosystems but is often reduced to copies of historical data[68]. Moreover, apart from this provision, there are currently no applicable horizontal legal rules allowing consumers to leverage data generated from the use of a connected product, e.g. by mandating the transfer of their data between different service providers. Thus, the exact scope of the existing portability right in data protection as well as the technical means ensuring interoperability are unclear. This is further aggravated by practical issues, such as delays in responding to the requests, incomplete files, and lack of machine-readable formats[69]. Consumers' ability to exercise their rights to data is tested on a case-by-case basis, as manufacturers generally do not offer interoperable formats and interfaces for standardised data exchange[70].

Smaller companies report that this complexity allows larger players to exclude access to data through technical and contractual means, e.g. dictate data formats (on unfair contractual terms see Driver 2). At the same time, technological means facilitating the

[67] European Commission (2022). *Outcome of the online consultation on the Data Act*.
[68] J. Cremer, Y.-A. de Montjoye, H. Schweizer (2019). *Competition policy for the digital era. Report of the Special Advisors to Commissioner Vestager*, p. 81.
[69] See this *presentation* from the ISA² Workshop; Drechsler, L. (2018). *Practical challenges to the right to data portability in the collaborative economy*, Proceedings of the 14th International Conference on Internet, Law & Politics, Universitat Oberta de Catalunya; J. Wong, T. Henderson, (2019). *The right to data portability in practice: Exploring the implications of the technologically neutral GDPR*, International Data Privacy Law, Vol. 9(3), p. 173.
[70] This is indicated by the annual inputs from the European Multi-stakeholder platform on ICT standardisation to the rolling action plan on ICT standardization, see *here*. See also Article 29 Data Protection Working Party (2016). *Guidelines on the right to data portability*; De Streel, A., Krämer, J. and Senellart, P. (2020). *Making data portability more effective for the digital economy*, CERRE Tech, Media and Telecom Study; Riechert, A. (2020). *Data portability*, Policy Paper.

automated and interoperable use of data, such as smart contracts, are hampered due to the absence of clear rules and standards[71].

A smart contract is a computer program on a distributed ledger with pre-determined conditions for the automated execution and settlement of a transaction of data, crypto assets, or services between autonomously operating machines. Smart contracts enable data holders to programme precise conditions for how, when and with whom else the recipient data are shared. Smart contracts linked to crypto digital assets also support escrow solutions that are needed to sanction a breach of conditions for data sharing. This makes smart contracts very useful for data sharing between entities that do not trust one another. Some 80% of the business respondents to the latest consultation confirmed their importance for data sharing and 55% affirmed they use smart contracts[72]. However, the lack of legal and regulatory clarity on this tool, lack of interoperability formats (especially regarding data portability) and high implementation costs impede their full potential from being harnessed.

With regard to competition law, the Horizontal Guidelines on the applicability of Article 101 TFEU on information sharing, and the evidence gathered in the ongoing evaluation, demonstrate that stakeholders lack guidance on new (digital) cooperation models. Information exchange is often mentioned in this regard, as cooperation in digital markets has expanded the possibilities to share and pool data[73].

Driver 2 – Abuse of contractual imbalances with regards to data access and lack of common data-sharing practices

Voluntary data sharing between businesses is typically based on contracts, concluded either only for the purpose of data sharing, as a part of an agreement between companies collaborating within the same supply chain or in the context of the purchase/ lease of a connected product or the supply of a related service. Where the contractual parties have aligned interests and share data, they create value from it and maximise benefits across the value chain.

Where the parties' interests are not aligned, some data holders either deny access to data altogether or offer data sharing only at abusive or excessive conditions, such as prohibitive prices[74]. The imbalance between the contractual parties, which provides the basis for this contractual behavior, stems typically from the fact that the party requesting access to data needs the data for developing or running innovative business models and can only get that data from a specific data holder. In such cases, the requesting party cannot create value from the data at all or only to a very sub-optimal extent.

[71] European Commission, Blockchain Strategy *webpage*; European Blockchain Observatory and Forum (2019). *Legal and regulatory framework of blockchain and smart contracts*; European Commission (2022). *Smart contracts and the digital single market through the lens of a 'law + technology' approach*, study prepared by Schrepel, T.; European Commission (2022). *Outcome of the online consultation on the Data Act*.
[72] European Commission (2022). *Outcome of the online consultation on the Data Act*.
[73] SWD(2021) 103 final, p. 75.
[74] Deloitte (2017). *New technologies case study: data sharing in infrastructure*. *A final report for the National Infrastructure Commission*.

Apart from the typical imbalance between data-haves and data-have-nots, situations where a data requestor is in a stronger negotiating position and abuses its bargaining power to the detriment of the data holder cannot be excluded either. Imbalances in negotiating power were raised in several sectors (e.g. construction, manufacturing, agriculture) and in cross-sectoral commercial activities (e.g. crafts), as confirmed by studies and the public consultation on the Data Act[75]. A recent study confirmed that contractual imbalances between data holders and data requestors affect, in particular, SMEs and start-ups[76]. The most prominent unfair terms detected by the study relate to the exclusion or disproportionate limitation of warranties and liability of the data holder, restrictions of data access and use, lock-in effects and conditions surrounding the termination of a data-sharing contract[77]. Such terms reduce the economic value of the data for the weaker party or deter data requestors from entering into a contract at all. The public consultation on the Data Act indicated that microenterprises and SMEs ranked 'unfair contract terms' second amongst the main difficulties for companies when requesting access to data. Further examples of the concrete problems related to the contracts are given in Annex 11.

Beside the issues linked to contractual imbalance there is also little established market practice for data sharing within sectors, and even less so across sectors, in the EU internal market. A few sectors have developed or are currently developing market practices for B2B data sharing, such as the codes of conduct in agriculture[78] and the legal guidance on industrial data in the technology/ manufacturing sector[79]. The DGA will further foster data sharing by providing rules on the structures and trusted mechanisms.

In some cases, mandatory data access rules set in sectoral legislation drive data-sharing and use practices. However, these exist only in very few sectors (e.g. banking, automotive, chemicals, electricity[80]) and conditions for access vary considerably. This leaves market participants in other sectors as well as those working across sectors without clear and consistent guidance on data-sharing conditions. Actors affected by legal uncertainty around data access or contractual issues are often deterred from seeking clarity by lengthy and costly court proceedings. This is especially the case in situations where a SME is involved against a larger company, as they lack the necessary resources.

Driver 3 – Lack of efficient rules and mechanisms for public sector bodies using business data in exceptional situations

[75] European Commission (2018). *Study on emerging issues of data ownership, interoperability, (re-)usability and access to data, and liability*, study prepared by Deloitte; European Commission (2022). *Study on model contract terms and fairness control in data sharing and in cloud contracts and on data access rights*, prepared by ICF; European Commission (2022, *forthcoming*). *Outcome of the online consultation on the Data Act*.

[76] European Commission (2022, *forthcoming*). *Study on model contract terms and fairness control in data sharing and in cloud contracts and on data access rights*, study prepared by ICF [section 2.2].

[77] Ibid, [section 6.2.2].

Companies produce and collect increasing amounts of data, the importance of which goes well beyond the private sector. The difficulty in accessing such data can affect the efficient functioning and timely response of public services. This problem was highlighted in the report of the High-Level Expert Group on B2G data sharing[81] and confirmed by 68% of the public authorities that replied to the online consultation. It was also recognised in a recent call to build a data infrastructure and ecosystem to tackle societal and environmental threats, endorsed by more than 400 signatories[82].

At the same time, the private sector is confronted with an increasing risk of inconsistent rules in the EU. Some Member States, for example France and Finland, have adopted horizontal or sector-specific legislation providing for public sector reuse of data held by businesses[83]. The current situation is likely to lead to fragmentation across multiple dimensions, including the type of data that can be collected, the manner in which it should be collected and the purposes for which this can be done[84].

Similarly, there are no binding rules about how collaborations should be set up, so businesses do not know what to expect in terms of scope of requests, licensing or charging possibilities. Problems signalled during the online consultation are the lack of safeguards ensuring that the data will be used only for the public interest purpose for which it was requested (75.7%), lack of appropriate infrastructures (64.2%) and lack of incentives (62.2%)[85].

The absence of a cross-border framework is particularly visible in the case of societal challenges which require cross-border and cross-sectoral datasets to be faced (e.g. environmental issues, containment of epidemics)[86] and whenever companies are confronted with requests from public sector bodies of different Member States for the same dataset. A stakeholder summarised the problems for businesses, *'which are called upon to comply with conflicting EU, national and local regulations, with more than often a duplication of similar requests among public authorities'*[87].

Driver 4.1 – Unfair market practices and vendor lock-in in cloud and edge services

Current practices of cloud and edge providers impede a fair and open market and hamper innovation, having an impact on data use across the economy. In particular, contractual, economic, and technical hurdles are currently preventing users to switch from one provider to another by porting their digital assets across. This problem of 'vendor lock-

[81] European Commission (2020). *Towards a European strategy on business-to-government data sharing for the public interest*, Final Report of the High-Level Expert Group on B2G Data Sharing.
[82] ODI, The GovLab, Cuebiq (2021). *The use of mobility data for responding to the COVID-19 pandemic.*
[83] See the French *LOI n° 2016-1321 du 7 octobre 2016 pour une République numérique* and the *Finnish Forest Legislation*.
[84] European Commission (2022). *Study to support an Impact Assessment on enhancing the use of data in Europe*, by Deloitte.
[85] European Commission (2022). *Outcome of the online consultation on the Data Act*.
[86] European Commission (2020). *Towards a European strategy on business-to-government data sharing for the public interest*, Final Report of the HLEG on Business to Government Data Sharing.
[87] Position paper of EU Travel Tech, see European Commission, Have you Say *webpage*.

in' has significantly intensified over the last decade[88]. It is aggravated as a result of the current trend whereby providers increasingly offer different types of cloud services in an integrated ecosystem, preventing customers from using other providers. Such ecosystems often turn into 'data siloes' that hamper the open character of the data processing market and the adoption of innovative data sharing tools.

The Free flow of non-personal data Regulation introduced a self-regulatory approach to address this problem, by encouraging industrial stakeholders to develop codes of conduct for easier cloud switching[89]. Following a difficult self-regulatory process that missed the regulatory deadline, the resulting 'SWIPO' codes of conduct were presented by mid-2020. Since then, only 16 cloud services of 8 providers have signed up[90]. This is a very small number, considering that one specific provider already offers two hundred different cloud/edge services[91].

The Commission has performed two evaluation procedures of the SWIPO codes of conduct. One consists of three legal assessment reports of the codes, conducted by independent law firms tasked to evaluate their effectiveness compared with the requirements posed by the Free flow of non-personal data Regulation (see Annex 9)[92]. The other is a support study for the Commission evaluation of the Free flow of non-personal data Regulation. This study is currently ongoing.[93] Aside from evaluation studies, the numbers indicate that the industry's proposed codes do not comply with the requirements of the Regulation: they are largely limited to an approach of pre-contractual transparency, instead of addressing also technical and economic hurdles as required by the Free flow of non-personal data Regulation. As a result, the SWIPO codes will not be sufficient to have a positive impact on the cloud market dynamics.

In addition to vendor lock-in, European businesses are also encountering other problems related to unbalanced contracts. A recent study[94] evidenced that 582 924 micro companies and SMEs in the EU have encountered contract-related problems while using cloud computing and have consequently faced a loss of turnover and profits.

Driver 4.2 – Access to data that is potentially in conflict with EU or national law affects the trustworthiness, security, and privacy of the data economy

The trustworthiness of cloud services equals the trustworthiness of the data economy: when data are shared from one actor to another, they mostly remain stored/processed in a

[88] See the relevant academic literature on this: D. Arce (2020). *Security-Induced lock-in in the cloud*, see *here*; D. Angamuthu & N. Pandian (2020). *A study of the cloud computing adoption issues and challenges*, see *here*; K. Varonen (2021). *Perceived development experience with cloud services: how an organization should decide between emerging cloud products*, see *here*; T. Debbarma, K. Chandrasekaran (2020). *A review on mobile cloud computing interoperability issues and challenges*, available *here*.
[89] OJ L 303, 28.11.2018, p. 59–68.
[90] SWIPO (2021), see *here.*
[91] See What is AWS *webpage*.
[92] European Commission (2021, *attached*). *Preliminary assessment reports on SWIPO IaaS and SaaS Codes of Conduct*, prepared by law firms Arthur Cox, Dorda and Ramon y Cajal.
[93] European Commission (2022). *Interim report on SWIPO Codes of Conduct*, prepared by Deloitte.
[94] European Commission (2019). *Study on the Economic Detriment to Small and Medium-Sized Enterprises Arising from Unfair and Unbalanced Cloud Computing Contracts*.

cloud environment. Where trust issues persist regarding unlawful access to those cloud environments, this directly encompasses the whole data economy built on top. In that sense, the issue of trust underpins all other interventions proposed by the Data Act.

The most problematic driver behind the trust problem relates to unlawful access to data by authorities not subject to EU legislation. There are situations where EU and third country authorities have a legitimate interest to access data, in particular in the framework of criminal proceedings and where there are reciprocity agreements in place[95]. However, cloud and edge services provided in Europe may receive requests to access data from non-EU/EEA authorities that are in conflict with EU or national data protection laws. Commercially sensitive data of a non-personal nature are specifically vulnerable in this regard, as they are not covered by the EU data protection framework (as opposed to personal data). This restrains the full potential of the data economy in Europe. In fact, stakeholders report reluctance to use cloud services due to concerns of unlawful or unauthorised access that may lead to IP theft, industrial espionage or the data being transferred to third countries that lack appropriate safeguards (such as enforceable rights and effective legal remedies)[96].

In this regard, specific laws with extraterritorial effect of several third countries have raised concerns among European citizens and businesses[97]. Through these laws, the third country may oblige certain cloud and edge service providers to grant its authorities access to data from EU organisations that are customers of the cloud providers, even if this data is processed in the EU. Moreover, in some cases it is prohibited for cloud providers to notify their customers of this data access[98].

To illustrate the scale of the number requests under the aforementioned laws, without being able to measure the degree of extraterritoriality of those requests, the number of government requests for access to customer/enterprise data that the three largest cloud service providers received globally between July and December 2020 totalled 389 776, affecting a multiplicity of accounts globally. Each of the three largest players also received requests under the Foreign Intelligence Surveillance Act (FISA), affecting a minimum of 109 500 accounts globally. It is unclear how many of these requests covered data from European businesses and citizens.

In a recent letter[99] on the subject of cloud security certification, the European Data Protection Board (EDPB) acknowledged the importance of this problem, stating '*specific criteria [are needed] to ensure protection against threats represented by access from authorities not subject to EU legislation (…). Failing to do so would be a missed*

[95] COM/2018/225 final - 2018/0108 (COD).
[96] European Commission (2022). *Study to support an Impact Assessment on enhancing the use of data in Europe*.
[97] By way of example: Executive Order 12333 (US), Section 702 of the Foreign Intelligence Surveillance Act (FISA) (US), The US CLOUD Act (US), the 2017 National Intelligence Law (China) and more.
[98] The USA FREEDOM Act of 2015 requires service providers targeted by FISA to delay any reporting by 6 months and report in bands of 500. Major providers adhere to this requirement - see e.g. *this*, *this*, and *this* for the reports from Apple, Microsoft and Amazon respectively.
[99] EDPB (2021), Letter of 18 November 2021 to ENISA regarding the European Cybersecurity Certification Scheme for Cloud Services, see here.

opportunity to foster security and compliance across Europe.' In the letter, the EDPB specifically states that the aforementioned threat affects not only personal data but 'all kinds of information'.

Driver 5 – No common standards for reusing data within and between sectors

The OECD notes that *'one of the most frequently cited barriers to data sharing and reuse is the lack of common standards, or the proliferation of incompatible standards'*[100]. In a study conducted by Everis on data sharing, technical interoperability was the most frequently cited obstacle (73% of companies)[101]. This is confirmed by the 2020 public consultation on the European data strategy, where 92% of respondents agreed that standardisation is necessary to improve interoperability and ultimately data reuse across sectors. Some 91% of respondents agreed that future standardisation activities need to better address the use of data across sectors of the economy or domains of society[102]. This cross-sector standardisation need is confirmed by a study indicating that depending on the sector, between 20% and 36% of the benefits of data sharing come from sharing between sectors and from diverse sources[103].

Data can only be used and reused, and generate value in different contexts, sectors and within the Internal Market, where the actors involved understand and trust the interfaces mediating data access. This 'interoperability', in the form of common and compatible standards to describe data semantics and data formats etc., is, amongst other things, essential to the functioning of common European data spaces[104] and to ensure the flow of data between data spaces, in order to prevent the appearance of silos. The 2019 series of workshops on common European data spaces[105] highlighted several issues regarding standardisation within different sectors.

The absence of common standards is also a very relevant problem for the effective portability of data and for switchability between cloud and edge services. It is the most important technical cause of vendor lock-in in cloud and edge services, particularly as regards services that go beyond simple storage (PaaS/SaaS)[106]. Different data formats, data semantics or data architectures lead to different outcomes on the basis of the same data, and this prevents a specific application after switching from being maintained. While technical interoperability of simple storage (IaaS) cloud services may be easier in theory, at the SaaS level it forms a prohibitive obstacle. That is why standardisation efforts could offer a solution also for cloud and edge service interoperability.

[100] OECD (2019). *Enhancing Access to and Sharing of Data; Reconciling Risks and Benefits for Data Re-use across Societies*, OECD Publishing, Paris.
[101] Everis (2018). *Study on data sharing between companies in Europe*, Study prepared for DG CNECT.
[102] European Commission (2020). *Outcome of the online consultation on the European strategy for data*.
[103] Deloitte (2018). *Realising the economic potential of machine-generated, non-personal data in the EU*, Report for Vodafone Group, p. 32.
[104] European Commission (2019). *Reports of the workshops on common European data spaces*.
[105] Ibid.
[106] European Commission (2018). *Switching of cloud services providers*, prepared by IDC and Arthur's Legal.

2.3. How will the problem evolve?

In **B2B contexts**, it is expected that the disparity in negotiating power between companies engaging in data transactions and lack of clarity over data and uncertainty as to IP rights will persist or deepen. The increasing complexity of data value chains makes businesses increasingly reluctant to provide access to their data for reuse, with negative effects for innovation and added value creation. For instance, due to insufficient data use, only 10 to 20% of the potential value of data generated in the financial sector is currently accessible[107]. Data-driven network effects and associated entry barriers in fast-evolving digital markets will continue to drive innovative start-ups out of aftermarkets, negatively affecting new business models, in particular those based on data, e.g. AI analytics and advanced data-driven services such as predictive maintenance[108]. A UN study predicts that, with the inherent dynamics of the data economy, companies currently leading the 'data race' will make it difficult for smaller firms to compete[109], potentially depriving customers of lower prices. Furthermore, the absence of standards for data sharing will limit communication and sharing between different data spaces, potentially duplicating efforts in obtaining data across sectors.

In **B2C contexts,** practical limitations (such as the insufficient level of interoperability) to exercising the rights to port all data generated by the use of products will hamper consumer choice for digital products and services[110]. Consumers will continue to be locked into certain service providers due to the high switching costs, which will limit demand for competing products and services, with knock-on effects on innovation[111].

In **B2G contexts**, public sector bodies and European institutions are likely to continue to be unable to reuse the data necessary for responding in a harmonised way to challenges at local, national and EU level, and in tackling cross-border emergencies. Companies are likely to continue facing uncoordinated requests for data. As some Member States continue to adopt different rules and administrative practices (e.g. justification for data disclosure requests or compensation rules), this will generate increasing inefficiencies and competition issues in the single market).

The problems related to **cloud and edge services** are likely to persist without policy intervention. The self-regulatory SWIPO codes of conduct do not address technical or economic hurdles to interoperability but are limited to a pre-contractual transparency approach. The Digital Markets Act focuses on data portability (not broader switching) for gatekeepers. As vendor lock-in can only be tackled by addressing the contractual, technical and economic problems together, vendor lock-in practices in cloud and data services are expected to persist. Several respondents to the online consultation indicated that codes of conduct should be granted more time to mature, be properly implemented

[118] McKinsey Global Institute (2021). *Financial data unbound: The value of open data for individuals and institutions*.
[108] JRC (2018). *Access to digital car data and competition in aftersales services*, Digital Economy Working Paper 06.
[109] UN (2019). *Data economy: radical transformation or dystopia?* UN Frontier technology quarterly.
[110] A concern shared by the European Consumers Association in the 2020 consultation on the data strategy.
[111] Borghi, M. (2019). *Data portability and regulation of digital markets*, CIPPM.

and gain the confidence of cloud actors. This view is counterbalanced by several cloud user organisations who stated that the codes of conduct will have a limited impact on the market[112]. As regards potential unlawful access to data, the concerns of stakeholders are likely to continue to intensify, as studies show that the dependence of EU businesses on cloud services is growing, and that the market share of non-EU/ EEA hyperscale providers is growing in Europe, despite private industrial initiatives such as 'Gaia-X'[113].

3. WHY SHOULD THE EU ACT?

3.1. Legal basis

This initiative is part of the European strategy for data. It intends to complete the single market for data[114]. Data-driven products and services are often developed using data from different Member States and later commercialised across the EU. Existing legislation already ensures the free flow of personal and non-personal data across the internal market. The development of a comprehensive framework to access and use data, will complement these measures to allow the full potential of the internal market in relation to the data economy to be achieved. With a growing digitalisation of the economy and society, there is also a risk of Member States legislating data-related issues in an uncoordinated manner, which will lead to fragmentation in the internal market.

Accordingly, Article 114 TFEU is the appropriate legal basis for this initiative.

3.2. Subsidiarity: Necessity of EU action

Data economy is an integral part of the EU internal market: in the EU, key sectors of the economy span across borders, with suppliers, producers and clients established in different Member States. Data flows form an intrinsic part of digital activities, and they mirror existing supply chains and collaborations. Any initiative aiming to organize such data flows must address the whole EU single market.

Datasets in individual Member States often do not have the richness and diversity needed to allow big data pattern detection or machine learning. Moreover, many of today's societal challenges, such as health crises and environment-related extreme events, are of a cross-border nature and therefore require data from across the EU in order to address them. In addition, data-based products and services developed in one Member State may need to be customised to the preferences of customers in another, and this may require local or even international data.

The market and regulatory failures identified in Chapter 2 are not Member State-specific: in the single market, potential obligations on manufacturers of connected products, for both personal and industrial use, can only be set at EU level. Similarly, cloud providers

[112] Contributions of Beltug, CIGREF, CIO Platform The Netherlands, VOICE to the online consultation on Data Act. They represent the Chief Information Officers of hundreds of mostly large (but also some smaller) businesses from Belgium, France, Germany and the Netherlands.
[113] Infotechlead (2021). *Amazon, Microsoft and Google grab cloud share in Europe*; and *here*.
[114] Area in which data from the public sector, businesses and citizens can be accessed while respecting rights in relation to such data and investments made into their collection.

usually place general service offerings on the market at EU level, without distinguishing between Member States. Poor switchability strengthens the dependence of European cloud users (e.g. software developers on non-EU service providers) and promotes the appearance of inefficient data silos across the internal market. The identified problems related to cloud and edge services therefore require a transversal EU solution. Fairness of B2B (data-sharing and cloud) contracts would be difficult to achieve through different national rules which could allow the party with the strongest bargaining power to choose the applicable law with the lowest level of protection. The cross-border nature of industrial data value chains, of cloud computing service offers and of the production and sales of connected products makes it very difficult to address problems of fairness related to contractual rules on data sharing, access and use at Member State level.

Moreover, the clarification of the role of the *sui generis* database right and its relationship with machine-generated data cannot be achieved by Member States alone. This right is part of the *acquis* and is an autonomous concept under EU law. It therefore requires a review of the Database Directive.

The Commission indicated in 2018 that it would consider legislation to address obstacles to data use in the single market in case of their persistence[115]. In the context of the growing economic impact of IoT globally, EU rules are best suited to maximise the socio-economic value of IoT data while taking account of the existing national differences and interests. At the same time, Member States are already launching B2B data sharing initiatives, such as the Dutch Data Sharing coalition[116], the Smart Data Initiative in Germany[117] or the data contracts initiative of the Technology Industries in Finland[118]. Such developments might privilege national data champions, without due regard to the balanced development of the overall EU data market. Similarly, some Member States have adopted horizontal, or even sector-specific legislation concerning B2G data sharing. In France, for example, the law for a digital republic allows the public sector to access certain private sector data of general interest, i.e. data necessary for official statistics[119]. In Finland, the Finnish forest act obliges forest owners to share information related to the management of the forest (such as forest utilisation, damage etc.) with the public sector[120].

EU intervention, unlike national intervention, can ensure a coherent framework in the single market[121] for national as well as sectoral approaches to tackling data barriers, and ensure comparable access and use conditions for common European data spaces.

[115] COM/2018/232 final.
[116] https://datasharingcoalition.eu/
[117] German Federal Ministry for Economic Affairs and Energy (BMWi), *Smart Data – Innovations in Data* (2016), available *here*.
[118] See *here*.
[119] French legislation, *Loi No 2016-1321 du 7 octobre 2016 pour une République numérique*.
[120] Ministry of agriculture and forestry of Finland: Forest legislation in Finland, see *here*.
[121] Max Planck Institute for Innovation and Competition, *Arguments against "data ownership"*.

3.3. Subsidiarity: Added value of EU action

Considering the importance of economies of scale for the development of data technologies and services, coordinated action at EU level can bring greater value to the European economy and society as compared to action by individual Member States. The data value chains in the EU are already structured largely in a cross-border manner, with data holders, data enrichers and final data users scattered across various Member States.

Stakeholder consultations have confirmed that the main obstacles to data access and use are neither country- nor sector-specific. On the contrary, problems of a legal, technical, and economic nature persist across the entire EU market[122]. In addition, the other key elements of the legal framework applicable to the EU data market are also EU level instruments (GDPR, ePrivacy Directive, Open Data Directive, DMA and DGA proposals). Concerted EU action is a therefore the most efficient manner of achieving a functional and coherent common data space.

4. OBJECTIVES: WHAT IS TO BE ACHIEVED?

4.1. General objective

The Data Act's general aim is to maximise the value of the data in the economy and society by ensuring that a wider range of stakeholders gain control over their data and that more data is available for use, while maintaining incentives for data generation and collection.

4.2. Specific objectives

The specific objectives of the intervention are formulated in response to the main problem areas identified in Chapter 2, as shown in the figure below.

1. Empower consumers and companies using connected products

In the context of the rapid development of IoT technologies and an increased deployment of connected products, the Data Act would aim at allowing users of such products and related services, particularly consumers and SMEs, to participate more in the data economy. They should therefore have access to the data their connected product collect and be able to choose to give a third-party access to such data for reuse. This requires clarifying the legal framework on data access, increasing transparency on what data is being created, ensuring that charges for access are not used to discourage data access and addressing the risks related to the abuse of strong bargaining position.

2. Increase availability of data for commercial use and innovation between businesses

Businesses should be incentivised to establish consistent and balanced data sharing practices across sectors on the basis of a set of clear rules as to who can access and use what data that are applicable across all sectors and under which conditions. To ensure a

[122] European Commission (2022). *Outcome of the online consultation on the Data Act*.

proactive role of businesses in the data economy, it is also important that entities that have invested in data generation continue to be fairly rewarded for these investments and are shielded against an increased risk of unlawful access to data. Companies with a weak bargaining position need to be shielded from the abuse of contractual imbalances by parties with a significantly stronger bargaining position.

3. Introduce new mechanisms for reuse by public sector bodies of data in exceptional situations

Public sector bodies should be able to reuse data necessary for carrying out their tasks in exceptional situations. When pressing data needs cannot be addressed by the current mechanisms, new B2G data reuse arrangements should maximise the benefits for society while minimising the burden on businesses, especially SMEs.

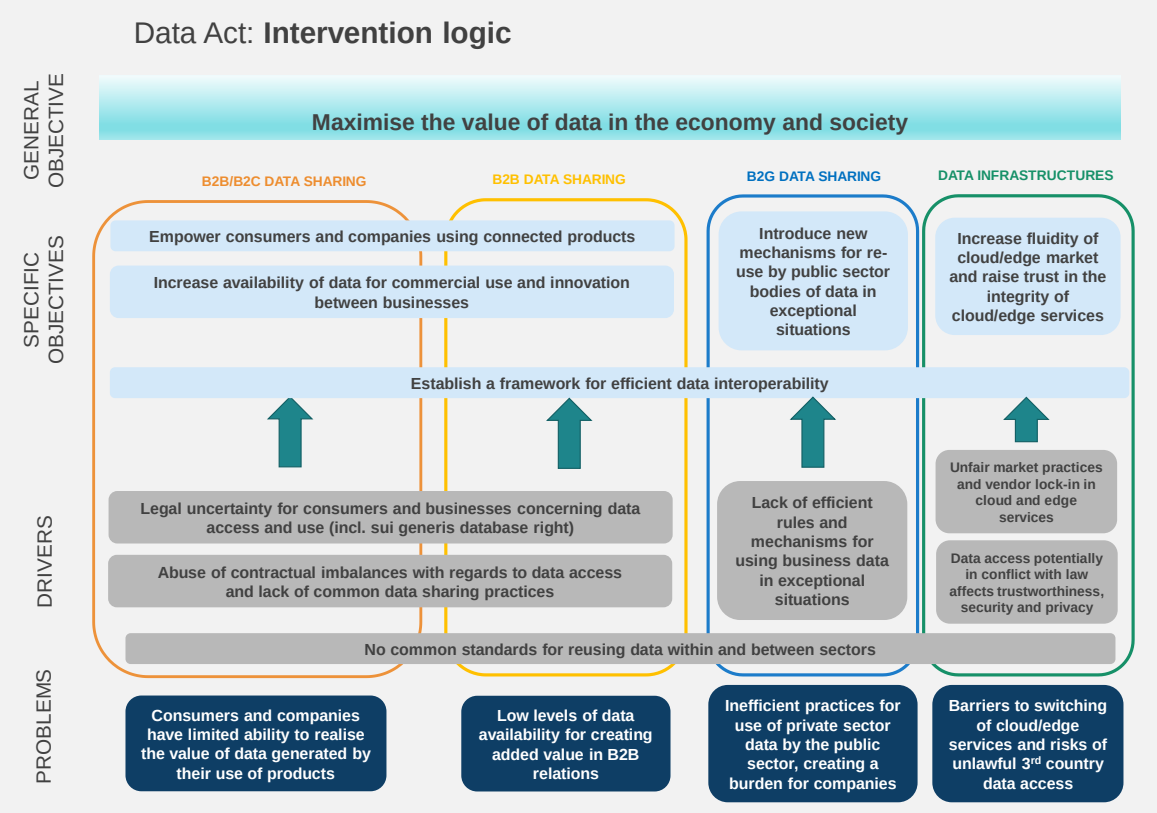
4. Increase the fluidity of the cloud/edge market and raise trust in the integrity of cloud and edge services

To guarantee operational control over data and to facilitate the use of future-proof and innovative tools for data access and use, cloud users in the EU should have access to fair and trustworthy cloud services, regardless of the home jurisdiction of the service providers. By taking away barriers to switching on the cloud market, the cloud offering in Europe should be brought in line with Europe's innovation needs: the emergence of a fully interoperable and vendor-agnostic (often federated) cloud and edge continuum.

5. Establish a framework for efficient data interoperability

Minimum common principles and standards should allow actors across sectors to access, port data and to create value efficiently from data coming from different sources. This should reduce transaction costs[123] and enable actors to find the high-quality data they need so that data can be reused across sectors and common European data spaces. The needs and existing standardisation actions for individual sectors and data spaces and the set-up of the respective stakeholder ecosystems will be fully taken into account[124].

[123] Increased interoperability greatly reduces the costs of data 'pooling'. See Carballa Smichowski, B., Duch-Brown, N. & Martens, B. (2022). *To pool or to pull back? An economic analysis of health data pools*, JRC Digital Economy Working Paper.
[124] SWD(2020) 295 final.



5. WHAT ARE THE AVAILABLE POLICY OPTIONS?

In line with the objectives of this initiative, the policy options are designed to realise the vast socioeconomic potential of data use which is currently underexploited along the value chain, both for data holders and data re-users as described in Chapter 2.

The overall approach, coherent with the wider European strategy for data, is that qualified obligations should apply only where strictly necessary to tackle clear, major imbalances and data bottlenecks. .

Levers have been identified to achieve this through the debate on data access and use over recent years. In B2B and B2C relations, these levers include: scope of rights and obligations regarding data; product design affecting how easily data can be accessed; conditions and compensation for data access; adjusting imbalances in businesses' bargaining power in contractual relationships; standards for promoting interoperability. In the B2G context, they include the conditions and the extent of use of companies' data by the public sector. For cloud services, they include contractual and technical measures to enable switching in practice.

Three policy options have been developed, each of which combines several levers with different emphases and levels of intensity in terms of widening access and use of data that currently remain under de facto exclusive control of the data holders. Each option builds on earlier analyses and discussions with stakeholders, and each would be realistic and reasonable to implement.

- Policy option 1 focuses on preserving existing incentives to invest in data generation. It aims to nudge data holders towards facilitating more voluntary data access and use, with minimal intervention and only non-binding measures which do not necessarily remove data holders' often exclusive control over data.
- Policy option 2 (legislative option) aims to balance existing incentives to invest in data-generating activities with legislative measures that strengthen legal certainty on how data can be used and by whom, along with a light regulatory approach defining minimum framework conditions for switching between cloud and edge providers.
- Policy option 3 (legislative option) would boost innovation through data use by means of stricter conditions on data holders with regard to compensation, and by imposing detailed technical specifications for data access. It also specifies detailed technical standards for ensuring cloud interoperability.

None of the options affect existing applicable rules on data protection, privacy, intellectual property (with the exception of changes introduced by the review of the Database Directive), competition, justice, and home affairs and related (international) cooperation, nor do they affect the EU's trade obligations. They do not affect the legal protection of trade secrets, nor do they include a general obligation to disclose trade secrets. Each leaves room for more detailed interventions in specific sectors, if necessary, that complement the Data Act.

5.1. What is the baseline from which options are assessed?

5.1.1. Why two baselines are used in this Impact Assessment

The impacts of the policy options have been assessed against two baselines. This is because this Impact Assessment builds principally on two studies, one prepared by Deloitte and one by ICF, each of which has a specific scope. Due to this difference in scope, the studies use a different baseline and consider the impact on the most relevant stakeholder groups.

- The ICF study focuses on contractual agreements in B2B contexts. Therefore, its baseline ('ICF baseline') is based on the number of 'data companies' and on the revenues of data suppliers active in the data market.
- The Deloitte study looks more broadly into B2B (except in relation to contractual matters), B2C and B2G contexts. It considers a wider scope of affected stakeholders, including companies beyond those included in the data market (data suppliers and data users), consumers and data 'co-generators'. Its baseline ('Deloitte baseline') is therefore wider, as explained below.

As said above, the baseline used in each study is defined in relation to its scope which, in turn, determines the range of affected stakeholders. Each baseline is the most relevant to assess the associated impacts of the measure(s) in the specific context. While the two baselines, the scope of the studies and their corresponding stakeholder bases are distinct and independent in their character, the studies are complementary in assessing different aspects and issues for data access and use in the B2B context.

5.1.2. Deloitte baseline

Considering that the current initiative would affect a wide range of stakeholders in all sectors of the economy, the total GDP for the EU27 of around EUR 11.5 trillion in 2020 has been chosen as the most suitable baseline against which the impacts of different policy options can be measured[125]. The Deloitte baseline is expected to grow to around EUR 13.80 trillion (+20%) in 2028[126]. This calculation takes into account the impact of certain existing and planned data-sharing instruments (see section 1.3), in particular the DGA and the Digital Markets Act (DMA). It also takes into consideration other initiatives under the Data Strategy that would facilitate voluntary data sharing and promote the development of data spaces. With regard to the problem areas in scope of this initiative, the baseline scenario can be described as follows.

Large, integrated tech companies that have already collected vast volumes of data would continue to exploit data to launch new digital services, thus contributing to GDP growth. However, they would at the same time strengthen their ability to determine data access by users and third parties. This is likely to restrict data supply for innovative SMEs in the aftermarkets and to limit consumer choice. The resulting increasing imbalances in negotiating power would to a very limited extent be addressed by the DMA proposal in cases where a gatekeeper is involved, whereas data in individual sectors (finance, automotive, transport, electricity) could be shared in line with, and to the extent there is, applicable or upcoming sectoral legislation.

An association described the likely development as follows: *'Without legal regulation of data access, there will be no way to ensure a level playing field among providers and freedom of choice for consumers in the future'*[127].

In the absence of binding EU rules, Member States may adopt (as some have already done, see section 3.2) national or sectoral legislation on the reuse of businesses' data by public sector bodies, increasing over time the volume of data reused but potentially increasing legal fragmentation and the resulting costs for companies[128].

In the area of cloud and edge, few services are currently declared under the SWIPO codes of conduct, whose scope is very limited. Therefore the barriers to switching across the cloud market would persist over both the short and long term, especially for PaaS and SaaS markets, where SMEs and start-ups that build innovative solutions on top of PaaS services would be most negatively affected (they indeed currently need to redesign their systems when they try to switch)[129]. For example, the tools that app developers or website builders use are normally offered as a cloud service at the PaaS layer. They are

[125] See Annex 4, section 5, for the methodology used to determine the EU27 GDP.
[126] European Commission (2022). *Study to support an Impact Assessment on enhancing the use of data in Europe* (Section 3.5.2).
[127] Position paper of Allgemeiner Deutscher Automobil-Club (ADAC), sent in the context of the public consultation on the Data Act.
[128] European Commission (2020). *Towards a European strategy on business-to-government data sharing for the public interest*, Final Report of the High-Level Expert Group on B2G Data Sharing.
[129] European Commission (2018). *Switching of cloud services providers*, prepared by IDC and Arthur's Legal, p. 31.

often effectively locked into such cloud services as they are not able to edit their apps or websites using the tools of a different PaaS cloud service provider.

In addition, without additional safeguards to address the concerns about potentially unlawful access to data by non-EU/EEA authorities, a lack of trust in cloud and edge services would continue to hamper growth of the EU data processing sector.

5.1.3. ICF baseline (related to contractual issues)

The ICF baseline takes into consideration the amount of data-related profits. Value generated under data sharing is expected to grow under this baseline from EUR 21.3 billion p.a. to EUR 27.1 billion p.a. over the period 2021-2030[130] (see Annex 4). The estimation of the baseline starts from data on revenues from data companies from 2013 to 2020[131]. The starting point in calculating the estimates of the value of data sharing are the profits of data companies which are expected to increase even under the baseline. To overcome the challenge of the lack of data, the study chose to estimate the profits of data suppliers as a proxy for improving the situation on data sharing. This choice is based on the assumption that the economic situation of data suppliers likely evolves in the same way as the data economy as a whole. Section 8.1 shows that, while methodologies differ, the finding is consistent across comparable studies, including internationally.

5.2. Description of the policy options

This section describes the different policy options for addressing the identified problems. A **more detailed description of the measures** under the policy options (2 and 3) is presented in Annex 10.

5.2.1. Policy Option 1 – Non-binding measures encouraging wider and more efficient data access, use and processing among stakeholders

This option would consist of Commission guidance and supporting best practice and self-regulation among the relevant stakeholders.

i) To empower consumers and companies using connected products and related services, *the Commission would:*

- set up a forum of experts and stakeholders whose remit would be to create an industry-driven self-regulatory framework for 'co-generated data', i.e. data generated by machines and by the use of products and related services.
- This framework, such as a code of conduct per sector or across sectors, would aim for more consistency among sectors. It could include best practices for manufacturers in the application of the *sui generis* right under the Database Directive, and it could encourage allowing users of products to access data they co-generate.

[130] European Commission (2022, *forthcoming*). *Study on model contract terms and fairness control in data sharing and in cloud contracts and on data access rights*, prepared by ICF (Section 2.2.3).
[131] For the baseline, the ICF study relied on the most comprehensive and available dataset on data sharing and data-related revenues offered by the IDC Data Market Study (2020), see also Annex 4.

ii) To increase availability of data for commercial use and innovation between businesses, *the Commission would:*

- recommend a set of voluntary and balanced model contract terms on all data sharing, including for data generated by machines and users' products and related services, in order to promote know-how and facilitate B2B data use within and across sectors, in particular for the benefit of SMEs;
- elaborate non-binding recommendations on the use of specific standards for technical tools such as smart contracts.

iii) To introduce new mechanisms for reuse of commercially-held data by public sector bodies in exceptional situations, *the Commission would:*

support Member States in implementing the recommendations of the High-Level Expert Group on B2G data sharing, including on the setting up of governance structures to promote and oversee access to and reuse of data held by businesses.

iv) To increase the fluidity of the cloud/edge market and raise trust in the integrity of cloud and edge services, *the Commission would:*

- encourage industry to enlarge the scope and improve the content of the existing codes of conduct on switching and porting between cloud providers, and to supplement them by voluntary standard contractual clauses, which would transcribe the codes into contractual agreements. Any measures on interoperability would remain non-binding;
- not propose any regulatory intervention to enhance the trustworthiness of cloud and edge services subject to non-EU laws. Any intervention in this regard would remain voluntary, such as by cloud security certification or voluntary transparency registers.

v) To improve the interoperability of data, *the Commission would*

- adopt guidelines on the use of specific standards or technical tools useful in the context of data access and use.

5.2.2. Policy Option 2 – Rules on controlled and predictable data access and use

i) To empower consumers and companies using connected products and related services, *the Commission would introduce:*

- a new right for companies and consumer users to access data generated by their connected products and related services supplemented by measures to prevent users making manifestly unfounded or excessive or repetitive requests for the data;
- to avoid practical barriers to an effective data access, an obligation for manufacturers would ensure that data generated by connected products are easily accessible both by the product users and third parties (without detailed technical rules on how this access should be implemented in practice). They would also have to provide transparency towards users and third parties about what data are likely to be generated and how they can be accessed;

- an entitlement of third-party companies, upon the user's request, to access directly data generated by a user's product for providing added value services (i.e. any service the provision of which depends on or is improved by data coming from products, including repair, insurance or data analytics). Manufacturers would be able to (but would not be obliged to) require compensation for making data available. When compensation is sought, it should be limited to the share attributable to the individual request, taking into account the costs of setting up and operating of the necessary technical infrastructure and its maintenance where the data recipient is an SME, and prevent discrimination between comparable categories of data recipients. Where the recipient is a larger company, parties would have the margin to negotiate a reasonable compensation, including a return on investment in addition to the recovery of the costs of making the data available.[132] These rules on access to data generated by connected products and related services also frame the conditions for other types of data access obligations (see below under point ii) in order to avoid the risk of fragmentation in the future;
- to keep incentives in data generation, the manufacturer's possibility to access and use the data generated by the use of the connected product or related service remains unaffected;
- an explicit exclusion of machine-generated data from the scope of application of the *sui generis* right under the Database Directive: such data as a simple by-product of the main activity of a user of a product have potential value for the development of innovative products and services which is hampered by legal uncertainty about exclusivity of rights to use the data;

At the same time, the Data Act would introduce an exemption for small and micro manufacturers from these new obligations in order to keep the intervention proportionate and acceptable by stakeholders. Such entities would nevertheless remain subject to obligations to provide information and access to personal data in line with existing data protection rules.

ii) To increase availability of data for commercial use and innovation between businesses, *the Commission would introduce:*

- voluntary model contract terms (as PO1);
- an 'unfairness test' for B2B data sharing terms in contracts, including co-generated data, which addresses the issue of the abuse of imbalances in negotiating power in contractual relations. It would invalidate unilaterally imposed excessive contract terms on data access and use in 'take-it-or-leave-it' situations. The scope of the unfairness test would be limited to protecting SMEs as they are archetypically in a weaker bargaining position.[133]

[132] See Annex 10 for further details.
[133] See Annex 11 for further details, including on the functioning of the unfairness test in practice.

- general default rules on data access and use (including pricing), ensuring the cross-sectoral applicability of the act. Such rules would apply beyond the situations of data generated by connected products and related services, to situations where there is a legal obligation for data to be made available coming from other sectoral or horizontal legislation. These default rules would be in line with the access rules on data generated by connected products and related services above under point i);
- an obligation for Member States to establish dispute settlement bodies in relation to the general access rules for business-to-business relationships. This measure is intended to keep compliance burden in check and avoid unnecessary and more costly litigation before the courts.
- finally, to address the risk of misuse or misappropriation of data related to the obligation of making data available, the Data Act would introduce additional legal safeguards protecting data holders;

iii) To introduce new mechanisms for the reuse of commercially-held data by public sector bodies where there is an exceptional need to access and use that data, *the Commission would introduce:*

- a mechanism to enable Member State's public sector bodies as well as EU institutions and bodies to request and reuse data held by companies, on *ad hoc* basis, where justified based on exceptional need to use the data. These cover both the need to respond to public emergencies and in other exceptional situations where the public body requesting the data can demonstrate that the unavailability of data prevents it from carrying out of its core public tasks and at the same time the data needs cannot be met through available mechanisms (such as reporting obligations or procurement) and where setting new legal obligations would be inefficient due to time constraints or finally, where the different way of collecting the data would lead to substantial reduction of administrative burden for companies, replacing existing reporting obligations. Annex 10 describes the 'exceptional need' and the definition of 'public emergency' in more detail.
- harmonisation and legal certainty for businesses by not allowing Member States to use the B2G access right for ad hoc data access, as prescribed in the Data Act on grounds other than defined in the Data Act. This should be without prejudice to Union and national legislation obliging companies to share data in other situations and for other purposes (e.g. reporting or monitoring regulatory compliance);
- a mandate that, except for emergency situations, companies would be entitled to claim compensation that should not exceed the costs related to making the data available, and a reasonable return on investment (Annex 10 describes cost components in more detail);
- a requirement that each Member State has in place a competent authority to help streamline B2G requests, including cross-border requests as well as ensure compliance, including the power to impose fines

Finally, to keep the intervention proportionate and avoid imposing excessive administrative burden on SMEs, a general exemption of small and micro companies from B2G obligations would be introduced.

iv) To increase the fluidity of the cloud/edge market and raise trust in the integrity of cloud and edge services, *the Commission would introduce***:**

- a set of minimum regulatory requirements on cloud/edge switching, imposing framework conditions of contractual nature and governing applicable charges (more details in Annex 10). This should ensure that users can effectively switch their data and/or other assets between providers of cloud and edge services. To remain future-proof, policy option 2 would remain non-binding on technical aspects of interoperability (see the interoperability section below). This regulatory intervention would be lighter, albeit wider in scope, than the direct portability obligation of the Digital Markets Act to cloud providers that it designates as 'gatekeepers', which targets specific problematic services and may define how to enact portability;
- an obligation for cloud and edge providers to take reasonable technical, legal, and organisational measures to prevent potentially unlawful or unauthorised third-party access to data. This approach would be in line with Article 30 of the Data Governance Act (DGA), which has received wide support in the European Parliament and Member States. Since the Data Governance Act does not directly apply to cloud and edge services, the proposed approach would be to transpose in the Data Act the same provisions as DGA Article 30. The safeguards, in line with the EU's international commitments and trade policy, would be intended to make unlawful data transfer without notification by the cloud service provider impossible. The approach would be to set domestic requirements for services offered on the EU market, rather than targeting data transfers or flows to third countries (for which alternative measures already exist);
- an appropriate enforcement regime, by building on existing capacities in the Member States' national regulatory authorities (NRAs). As most cloud services are offered in a majority of Member States, NRAs would need to cooperate at European level. This could be done by establishing an EU-level coordination group on cloud governance.

v) To improve the interoperability of data and data processing services, *the Commission would introduce:*

- non-binding criteria for ensuring interoperability and respect for data access and use agreements between sectors through technical means, such as smart contracts and APIs;
- powers for the Commission to step in where insufficient progress has been made with EU-level standardisation processes and adopt common specifications for future proof and technologically-neutral interoperability and principles facilitating data use in common European data spaces, data portability and interoperability between particular types of cloud and edge services. In line with the Standardisation

Regulation, SMEs access to these processes would be ensured and the risk of dominance by bigger market actors minimised;

- a repository for cloud and edge interoperability standards to promote awareness and visibility of open standards and interfaces that technically enable switching of cloud and edge services, fully consistent with the forthcoming EU Cloud Rulebook[134].

The Data Act would not introduce new rules on sanctions but would instead rely on the Member States to indicate the appropriate existing sanction regime for the different types of relations addressed in the Data Act (to be applied by existing or newly created authorities, as deemed necessary).

5.2.3. Policy Option 3 – Rules for open data access between businesses and from businesses to public bodies

Policy option 3 proposes legislative measures to maximise the opportunities for parties to request access to data and determine how they can use it once available, with wider range of companies entitled to reuse data held by businesses, and a regime for B2G which emulates the approach of G2B under the Open Data Directive.

i) To empower consumers and companies using connected products and related services, *the Commission would introduce, in deviation from the measures under PO2,*

- an obligation for manufacturers to comply with common technical specifications, detailing how to enable data access by third party service providers (in terms of e.g. API requirements, formats, data latency, etc.) ;
- unlike policy option 2, no right for data holders to require compensation for the cost incurred in making data available to a third party at the user's request.

ii) To increase availability of data for commercial use and innovation between businesses, *the Commission would introduce, in deviation from the measures under PO2,*

- an unfairness test that would apply to all contractual terms – not only unilaterally imposed terms – on data access and use by all companies, not only SMEs;
- general default rules on data access and use, where there is a legal obligation for data to be made available not directly stemming from the Data Act. These default rules would be in line with the access rules on data generated by connected products and related services above under point i).
- unlike PO2, there would be no additional legal safeguards to protect data holders against misuse or misappropriation of data.

iii) To introduce new mechanisms for reuse of commercially-held data by public sector bodies, *the Commission would introduce, in deviation from the measures under PO2,*

[134] As announced in the European Data Strategy, the Cloud Rulebook will offer a compendium of existing cloud codes of conduct and certification on security, energy efficiency, quality of service, data protection and data portability. It will be published by Q2, 2022.

- a mechanism for public sector bodies to request reuse of data for any duly justified purpose;[135] there would be no requirement to demonstrate exceptional situations;
- in case of public emergencies, a provision for the data to be made available to public sector bodies and EU institutions and bodies free of charge; in other cases, at marginal costs for complying with the request;
- a requirement for public sector bodies and companies to designate a function ('data steward') responsible for handling B2G requests transparently and consistently[136]. This would follow one of the main recommendations of the high-level expert group on B2G data sharing.

iv) To increase the fluidity of the cloud/edge market and raise trust in the integrity of cloud and edge services, *the Commission would introduce, in deviation from the measures under PO2,*

- a direct and general switching obligation on cloud and edge service providers, effectively leading to a 'right to switchability' for cloud/edge users, regardless of the concerned cloud deployment model;
- binding technical requirements regarding the interfaces, data semantics and architectures to be deployed while users switch, defined by cloud service type.

v) To establish a framework for efficient data interoperability, *the Commission would introduce, in deviation from the measures under PO2,*

- data interoperability requirements in implementing acts, facilitating data use in common European data spaces, for data portability and for interoperability between particular types of cloud and edge services.

As under policy option 2, there would be no bespoke sanction rules.

5.2.4. Summary of policy options

Objective 1) Empower consumers and companies using connected products and related services (data covered: data coming from connected products and related services, including personal and non-personal)

[135] For details see Annex 10.

[136] See Data Collaboratives *website*; European Commission (2020). *Towards a European strategy on business-to-government data sharing for the public interest*, Final Report of the HLEG on B2G.

Policy Option 1	Policy Option 2	Policy Option 3
The Commission sets up a forum of experts and stakeholders to create a self-regulatory framework for co-generated data.	a) User right to access data from use of connected products and related services free of charge; Measures to prevent manifestly unfounded or excessive or repetitive requests for the data b) Obligation for manufacturers to ensure easy access as well as transparency requirement on OEMs regarding data likely to be generated and how it can be accessed c) Third party data access for providing added value services Compensation for making data available directly to a third party based on - a verifiable cost-based approach with an upper limit (for SMEs); - reasonable compensation without an upper limit(for larger companies) and - the principle of non-discrimination (for all) d) Exclude machine-generated data from the protection of *sui generis* right in Database Directive e) Exemption for small and micro companies	a) as PO2 b) as PO2 c) as PO2, supplemented with common technical specifications, detailing how to enable access (e.g. API requirements) No compensation d) as PO2 e) as PO2
Objective 2) Increase availability of data for commercial use and innovation between businesses (data covered: all types)		
Policy Option 1	**Policy Option 2**	**Policy Option 3**
The Commission supports the stakeholders by recommending non-binding balanced model contract terms on data sharing in B2B contexts (including machine-generated data) as well as on the use of specific standards for technical tools such as smart contracts	a) Model contract terms as PO1 b) Unfairness test to prohibit unfair conditions for data access and use regarding *unilaterally imposed contract terms* with SMEs c) General rules on data access applicable to any obligation to make data available, in line with the conditions of the data access right in objective 1) under c). d) Legal safeguards to protect data holders against misuse/ misappropriation e) Dispute settlement bodies	a) as PO2 b) Unfairness test applies *to all contract terms* c) No compensation, strict technical requirements d) No additional legal safeguards to protect data holders against misuse or misappropriation of data e) as PO2
Objective 3) Introduce new mechanisms for reuse of commercially-held data by public sector bodies (data covered: all types; mostly non-personal)		

Policy Option 1	Policy Option 2	Policy Option 3
The Commission issues guidance to support the Member States in the implementation of the recommendations of the B2G expert group report.	a) Mechanism for privately held data to be reused by public sector bodies if justified by an exceptional need b) Small and micro companies excluded from the new obligations c) Maximum compensation limited to costs plus reasonable return on investment, except in emergency situations where data is provided for free d) Member States have in place an institutional mechanism to streamline data requests, ensure redress and enforcement and to handle cross-border requests	a) Public sector bodies may request data for any duly justified purpose b) as PO2 c) Marginal cost compensation; free in emergencies d) as PO2 e) Businesses and the public sector required to designate data stewards to handle requests
Objective 4) Increase the fluidity of the cloud/edge market and raise trust in the integrity of cloud and edge services (data covered: all types)		
Policy Option 1	**Policy Option 2**	**Policy Option 3**
The Commission encourages industry to enlarge the scope and improve the content of the existing codes of conduct on switching and porting between cloud providers. Voluntary standard contractual agreements would supplement this.	a) Light regulatory approach focused on contractual aspects and charges, to facilitate switching by means of a minimum set of binding framework conditions. b) Cloud service providers obliged to take all reasonable measures to avoid third country access to non-personal data (personal data is covered by GDPR).	a) Direct and general switching obligation on cloud and edge service providers, leading to a 'right to switchability'. Detailed binding technical interoperability requirements b) as PO2
Objective 5) Establish a framework for efficient data interoperability		
Policy Option 1	**Policy Option 2**	**Policy Option 3**
The Commission adopts guidelines on the use of specific standards or technical tools useful in the context of data access and use.	Fall-back competence for the Commission to recommend common interoperability requirements or principles for selected common European data spaces, data portability and interoperability between cloud and edge services.	The Commission would lay down mandatory data interoperability requirements in implementing acts facilitating data use in common European data spaces, for data portability and for interoperability between particular types of cloud and edge services.

Annex 10 gives an overview of the scope of the measures in terms of the types of data in relation to their function and whether it concerns personal or non-personal data.

5.3. Options discarded at an early stage

No options were discarded at the outset.

6. WHAT ARE THE IMPACTS OF THE POLICY OPTIONS?

This section assesses the policy options in terms of their economic, social, and environmental impacts. It starts by focusing on the expected macroeconomic effects of

the three policy options. It then justifies those effects by explaining in detail the impact of the measures included in each policy option on the relevant groups of stakeholders. The section concludes with an examination of the possible non-economic effects on society and the environment.

6.1. Unleashing the value of data

As explained in Chapter 5.1., the impacts of the policy measures are assessed against two distinct, but complementary, baselines. Therefore, the impacts of the different intervention measures are considered separately.

- The Deloitte baseline, against which intervention measures related to B2B (except in relation to contractual matters), B2C and B2G are assessed, assumes that EU-27 GDP would reach EUR 13.80 trillion in 2028[137].
- The ICF baseline, against which intervention measures related to contracts in the B2B context are assessed anticipates that, on average, data-related profits for data suppliers would be around EUR 24.7 billion per year (2021-2030)[138].

The figures in this Chapter relate to costs and benefits as compared to the two baselines that would result only from measures taken under the Data Act. The costs and benefits resulting from sector-specific legislation are not considered here. Annex 4, point 1 provides more information on the key calculations and assumptions behind the figures.

Policy option 1 realises the lowest economic benefits compared to the Deloitte baseline, due to the fact that it depends on the uptake of voluntary measures. This adds a layer of difficulty in quantifying its impact[139]. Intervention in the area of contractual relationships is nevertheless expected to bring net benefits of EUR 5.4 billion p.a. to data suppliers[140].

In **policy option 2**, through intervention measures related to B2B and B2C (except contracts), EU-27 GDP could increase by EUR 273.1 billion, up to **EUR 14.07 trillion in 2028[141]**, equivalent to an additional 1.98% above the Deloitte baseline[142]. This figure considers the overall costs and benefits derived from the measures under this policy option. By 2028, investment activities are estimated to increase by EUR 30.4 billion[143]

[137] European Commission (2022). *Study to support an Impact Assessment on enhancing the use of data in Europe*, prepared by Deloitte (Section 3.5.2).
[138] European Commission (2022, *forthcoming*). *Study on model contract terms and fairness control in data sharing and in cloud contracts and on data access rights*, prepared by ICF (Section 2.2.3.2, Table 2.2).
[139] European Commission (2022). *Study to support an Impact Assessment on enhancing the use of data in Europe*, prepared by Deloitte (Section 3.3.1.3.2.).
[140] European Commission (2022, *forthcoming*). *Study on model contract terms and fairness control in data sharing and in cloud contracts and on data access rights*, prepared by ICF (section 8.3.3, Table 8.13 and. Annex 4, Table 4).
[141] European Commission (2022). *Study to support an Impact Assessment on enhancing the use of data in Europe*, prepared by Deloitte.
[142] This is calculated on the basis of the exact (non-rounded) figures in Section 3.5.2., Figure 34 of the European Commission (2022). *Study to support an Impact Assessment on enhancing the use of data in Europe*, prepared by Deloitte.
[143] Investment activity estimates are based on the investment rate, which is defined as the investment per value added at factor costs indicated as a percentage of the EU-27 GDP. According to Eurostat this investment rate is at 14.4% of the GDP.

and an additional 2.2 million jobs could be created[144]. Regarding contracts, additional net benefits of EUR 7.3 billion p.a. could be expected[145].

Under **policy option 3**, through intervention measures related to B2B and B2C (except contracts), EU-27 GDP could increase by EUR 221.0 billion, up to **EUR 14.02 trillion in 2028**, equivalent to an additional 1.60% above the Deloitte baseline[146]. By 2028, investment activities are estimated to increase by EUR 10.9 billion and an additional 800 000 jobs could be created[147]. Regarding contracts, net benefits of EUR 7.8 billion p.a. could be expected[148].

Table 1

Impact of measures related to B2B and B2C (except in relation to contractual matters) EU-27 GDP in 2028 (trillion EUR)		
Deloitte baseline	**Policy Option 2**	**Policy Option 3**
13.80	14.07 (baseline+EUR 273.1 bn)	14.02 (baseline+EUR 221.0 bn)

Table 2

Impact of measures related to contractual matters Net benefits for data suppliers (2021-2030) (billion EUR p.a.)		
ICF baseline	**Policy Option 2**	**Policy Option 3**
24.7	32 (baseline+EUR 7.3 bn)	32.5 (baseline+EUR 7.8 bn)

It should be kept in mind that the quantification of the economic impact presented above refers to the overall effect of the shift in the *status quo* from the current suboptimal situation in which data resources are not easily exploitable by device users, companies with low negotiating power, or the public sector. Detailed sector-specific cost/benefit considerations should be left to the various sectoral initiatives complementing this basic horizontal instrument.

Overall, enabling a wider access and use of data has the potential to make a significant, direct impact on the EU economy. This is corroborated by a study conducted by the

[144] European Commission (2022). *Study to support an Impact Assessment on enhancing the use of data in Europe*, prepared by Deloitte (Section 2.5.3.1.1, Figure 20 and Section 2.5.3.1.4, Figure 26).
[145] European Commission (2022, *forthcoming*). *Study on model contract terms and fairness control in data sharing and in cloud contracts and on data access rights*, prepared by ICF (Section 8.3.3, Table 8.13, Annex 4, Table 4).
[146] This is calculated on the basis of the exact (non-rounded) figures in Section 3.5.2., Figure 34 of the European Commission (2022). *Study to support an Impact Assessment on enhancing the use of data in Europe*, prepared by Deloitte.
[147] European Commission (2022). *Study to support an Impact Assessment on enhancing the use of data in Europe*, by Deloitte (Section 2.5.3.1.1, Figure 20 and Section 2.5.3.1.4, Figure 26). The lower impact of PO3 on GDP growth in relation to PO2 stems from the lower efficiency and productivity gains as well as higher costs of implementation of this option.
[148] European Commission (2022, *forthcoming*). *Study on model contract terms and fairness control in data sharing and in cloud contracts and on data access rights*, prepared by ICF (Section 8.3.3, Table 8.13., Annex 4, Table 4).

OECD (2019), which suggested that the induced impact for the wider economy generated by data access and use is 20-50 times higher than direct benefits[149].

The following sections present the impact of the different measures on the key stakeholder groups.

6.2. Impact on businesses

This initiative has the potential to significantly enhance the overall use of data by businesses. Increasing the available data resources will enable companies to transform those resources into value added services and products. This expectation is shared in the feedback received from various trade associations to the Inception Impact Assessment[150].

However, some companies will benefit more, while others will face new requirements and obligations. The positive impact on SMEs, who are the key beneficiaries of the Data Act, is described in detail in Section 6.3.

6.2.1. Intervention in B2B and B2C relations

The online public consultation shows that the majority of business associations and trade bodies favoured a cautious approach to compulsory data access and use. They argue that there are no serious problems in B2B data access and use or suggested non-binding remedies to address existing access obstacles, as a mandatory data access could negatively affect their incentives to invest in data generation. Large EU industrial players, including producers of connected products, software providers, telecom operators and publishers generally share this view.

On the other hand, associations representing farmers, insurance companies or the providers of repair and aftermarket services, in particular those in the automotive sector, are clearly in favour of binding measures obliging manufacturers to allow the access to the data they hold and enhancing data portability.

Around 60% of the stakeholders who responded to the public consultation endorsed the use of model contract terms[151].

6.1.1.1.<u>Policy Option 1</u>

i) Empowering consumers and companies using connected products and related services

To date, there is no evidence that existing non-binding measures related to data, such as the 2018 Commission guidelines on B2B or the codes of conduct developed by the agriculture industry, have led to significantly more data access and use[152]. Therefore, it is unlikely that policy option 1 would have a substantial impact on businesses (the impact on consumers is analysed in section 6.4.). Non-binding measures related to data sharing

[149] OECD (2019). *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies*, OECD Publishing, Paris, p.17.
[150] European Commission *Have your say webpage* on *Data Act & amended rules on the legal protection of databases.*

[151] European Commission (2022). *Outcome of the online consultation on the Data Act*.
[152] SWD(2018) 125 final; OJ L 134, 31.5.2018, p. 12-18.

would largely depend on the uptake by businesses of the Commission's recommendations or guidelines by Member States on such matters.

ii) Increasing availability of data for commercial use and innovation between businesses

Although also non-binding, the provision of model contract terms in the B2B context could, if adopted by stakeholders, lead to some benefits[153]. The use of model contract terms would increase B2B data sharing as they facilitate data sharing when the parties may be willing to share but lack know-how. They reduce legal costs, benefiting SMEs in particular[154]. The benefit from the use of model clauses under policy option 1 is expected to be around **EUR 5.38 billion p.a.** as compared to the ICF baseline for this intervention area, while estimated costs are around EUR 29 million p.a.[155] (see Annex 4). However, non-mandatory model contract terms would be of limited effect in addressing the imbalance of power in bilateral contractual relations[156].

6.1.1.2. Policy Option 2

Policy option 2 proposes a set of legislative measures to facilitate the access and use of data, while strengthening legal certainty on how data can be used and by whom as well as transparency on what data is being created. This option realises the greatest benefits for SMEs and consumers.

i) Empowering consumers and companies using connected products and related services

Facilitating access to and use of data generated by connected products and related services is expected to lead to efficiency and productivity gains of up to **EUR 196.7 billion p.a. by 2028**[157]. Data access will also reduce monopolistic structures in aftermarkets and increase the provision of services at lower prices.

Businesses and consumers using connected products and related services could see a reduction in costs linked to moving from one aftermarket service to another and new opportunities to use services relying on access to this data, amounting to savings of **EUR 68.1 billion p.a.**[158]. This takes into account the potentially reduced incentives for firms to collect data without being able to claim exclusive rights over them.

---

[153] Model contract terms have been shown to help B2B data sharing in the health sector, see: Carballa Smichowski, B., Duch-Brown, N. & Martens, B. (2022). To pool or to pull back? An economic analysis of health data pools. JRC Digital Economy Working Paper.

[154] European Commission (2022, *forthcoming*). *Study on model contract terms and fairness control in data sharing and in cloud contracts and on data access rights*, prepared by ICF (Section 8.2.3, Table 8.6). See section 6.3 for impact on SMEs.

[155] European Commission (2022, *forthcoming*). *Study on model contract terms and fairness control in data sharing and in cloud contracts and on data access rights*, prepared by ICF [section 8.3.3, Table 8.13 Modelled benefit per policy option].

[156] European Commission (2022, *forthcoming). Study on model contract terms and fairness control in data sharing and in cloud contracts and on data access rights*, prepared by ICF [section 8.2.3].

[157] Ibid. This is comparable to OECD study that estimates socio-economic benefits of an additional 1-2.5% of EU GDP, or an additional EUR 133 334.5 billion p.a., OECD (2019) CH 3. Economic and social benefits of data access and sharing in *Enhancing Access to and Sharing of Data; Reconciling Risks and Benefits for Data Re-use across Societies*, OECD Publishing, Paris, p. 1.

[158] European Commission (2022). *Study to support an Impact Assessment on enhancing the use of data in Europe*, prepared by Deloitte (Section 3.3.3.4.2.2, Table 80).

The smart home appliance sector, for instance, would benefit from the measures regarding access to data generated by connected products. This sector is categorised by obstacles to data use such as low levels of standardisation and impeded data portability, but a high number of market participants. Increased but predictable data access could unlock the high potential of such sectors, enabling more data use based on standards and allowing new players to join the market, thereby increasing consumers' choice.

Learning from the Payment Services Directive 2 (PSD2), mandating access to information on funds enabled market entry for certain third parties offering added value services. The Commission forecasted EUR 0.9-3.5 billion in savings to merchants as a result of PSD2. Early observations[159] indicate an increase in the number of start-ups and the appearance of a pan-European sector as a result of PSD2. A similar broad impact on competitiveness in aftermarket services linked to connected products and related services can be expected as a result of this policy option.

Manufacturers of connected products can expect their data to be used by a wider range of companies to prepare their own service offer (e.g. apps). Manufacturers may therefore benefit from a related widening consumer base for their products. They will also be able to continue exploiting data from products and rely on trade secrets protection, safeguards against unlawful data use as well as smart contracts to protect their sensitive data. However, they will have to respond to new requirements: for instance, they will no longer be able to assert their competitive advantage purely based on the exclusive control of data collected by products they manufacture. They are likely to face more competition in aftermarket services, in which their position so far was difficult to challenge.

Manufacturers of a connected product could incur costs related to compliance, including the development of data management agreements and document management systems, as well as to the technical infrastructure. However, the exact means for providing the access would not be prescribed. Therefore, the overall cost for providing the data under policy option 2 would be lower than in policy option 3, in which the exact technical means are specified.

The interviewed stakeholders estimated the amount of this cost to reach approximately EUR 1 million p.a. per large company (which, unmitigated and taking into account infrastructure costs, could lead to an average cost of EUR 5.8 billion p.a. between 2023 and 2028). However, this estimate seems to be a considerable overestimation because it is based on the need of elaborating complex data management agreements and of tracking the use of data downstream, which is not an obligation. Under policy option 2, the legal and technical safeguards benefitting the data holders would considerably automatize and facilitate the implementation and monitoring of the data agreements. Furthermore, in most cases, the technical adaptations necessary to allow the access to data would not need to be introduced 'from scratch' as it is likely that most of the larger

[159] SWD(2013) 288 final. Also Polasik M. *et al.* (2020). *The impact of Payment Services Directive 2 on the PayTech sector development in Europe*, Journal of Economic Behavior & Organization, Vol. 178, pp. 4.385-401.

companies (i.e. those covered by policy option 2) would already be well equipped and technologically ready to share data on a wide scale.

The costs for the development of technical solutions for the whole IoT market can be extrapolated from the Deloitte study's estimated costs for the fitness tracker market under policy option 2 – one-off and recurring costs of EUR 83.4 million and EUR 18 million p.a., respectively. Based on a reasonable assumption that only 25% of companies would choose to undertake this investment and considering that the fitness tracker market represents 5% of the EU IoT revenue, this implies a one-off and recurring costs of **EUR 410 million** and **EUR 88 million**, respectively, for the whole IoT market[160].

To address the negative impact of legal uncertainty and to ensure the effectiveness of the data access right, the ***Database Directive*** would be amended to exclude machine-generated data from its scope. Avoiding the undue IPR protection will allow machine-generated data to be re-used by a wider range of companies, fuelling innovation, and stimulating new use cases. Clarifying that the Database Directive *sui generis* right does not apply to machine-generated data will reduce costs related to: overly restricting access to and the use of such data, potential transaction costs, costs of opportunistic litigation, the risk of conflicting interpretation of the Directive's scope and diverging national implementations. Moreover, the exclusion of such data from the scope of *sui generis* protection is expected to ease access to complete datasets. This will facilitate the development of new value-added products and services and could contribute to increased revenues in the data supply chain. In addition, it is not expected to have a negative impact on the generation of data and databases in the IoT context[161]. However, some ***data holders*** (such as OEMs, for which use of their products generates data) may no longer be able to claim *sui generis* protection. Some ***legacy users*** of the Database Directive (e.g., in the publishing, media and broadcasting sectors) would not be affected: the type of automatically produced and processed data that those users rely on would not be targeted by this review.

ii) Increasing availability of data for commercial use and innovation between businesses

Model contract terms, complemented by a contractual unfairness test for unilaterally imposed unfair contract terms, and general rules for data access (i.e. rules that apply to data access rights beyond the Data Act) are expected to have a positive impact in terms of data-driven innovation, consumer surplus and productivity. The majority of the beneficiaries would be SMEs. By promoting data sharing at fair conditions, the benefits would outweigh potential legal and operational costs[162].

[160] The fitness tracker market was one of two representative markets for IoT products analysed in the support study. European Commission (2022). *Study to support an Impact Assessment on enhancing the use of data in Europe*, prepared by Deloitte (Section 3.3.2.4.2.1, Table 72).
[161] European Commission, (2022) *Study to support an impact assessment for the review of the Database Directive*, study prepared by CE-TP-CSIL-TU.
[162] See European Commission (2022, *forthcoming*). *Study on model contract terms and fairness control in data sharing and in cloud contracts and on data access rights*, prepared by ICF (Section 8.2.4).

By reducing the use of unfair contractual clauses and the abuse of a significant imbalance in negotiating position[163], the unfairness test would lower the barriers to data sharing. The general rules for data access would have a positive impact, as they are a more proactive and binding way to ensure the respect of fair principles in data sharing contracts[164].

The ICF study shows the expected benefit of these measures to be **EUR 7.4 billion p.a.**, compared to its baseline. However, as the ICF model is limited to the profits from data suppliers, and not the revenues of data users, the actual benefits can be expected to be considerably higher[165]. Additional direct and indirect benefits include reduced legal costs and reduced entry barriers for SMEs, and more resilient supply chains due to enhanced usage of data for the prediction of supply and demand. The estimated costs would amount to **EUR 69 million p.a.**[166].

The expected overall positive impact of the measures to improve contractual fairness was confirmed by the public consultation on the Data Act. It showed that almost half of the stakeholders across sectors (e.g. agriculture, construction, aftermarket, gaming, crafts, digital market) support an unfairness test (46%), which is more than double those not in favour (21%). SMEs show strong support (50%), and a significant number of large companies are in favour of an unfairness test (41%). Some respondents to the public online consultation, predominantly big players, considered contracts and competition law to sufficiently address the issue at stake. Also, on the general rules on data access, the public consultation on the Data Act shows support across sectors (e.g. aftermarket, digital, industry, gaming, financial): 46% agree, while only 20% disagree. While more than half of the responding micro and SMEs (52%) agree with this measure, a number of representatives from large companies also agree (41%)[167].

6.1.1.3. Policy Option 3

Policy option 3 proposes additional obligations in terms of the access and use of data by third party businesses, consumers, and public sector bodies. It also foresees stronger provisions in terms of obligations on data service providers and interoperability requirements and stricter conditions in terms of compensation. The main beneficiaries would be SMEs and consumers.

i) Empowering consumers and companies using connected products and related services

There would be an obligation on manufacturers under this option to set up technical infrastructures to comply with detailed specifications for ensuring access and portability of all data generated by the use of a connected product or service. This would create even better opportunities for the development of new services and products by third parties.

[163] Ibid.
[164] European Commission (2022, *forthcoming*). *Study on model contract terms and fairness control in data sharing and in cloud contracts and on data access rights*, study prepared by ICF [section 8.2.4].
[165] Ibid,(Section 2.2.3.2 and Annex 4).
[166] European Commission (2022, *forthcoming*). *Study on model contract terms and fairness control in data sharing and in cloud contracts and on data access rights*, study prepared by ICF [section 8.3.3, Table 8.13].
[167] European Commission (2022). *Outcome of the online consultation on the Data Act*.

Especially SMEs, would have more possibilities to compete and benefit from key information about supply chains, contributing to the establishment of new and complementary markets.

A reduction of costs related to easier shifting from one aftermarket service to another is expected to generate 20% cost savings for companies, amounting to **EUR 90.8 billion p.a.**[168]. Similar business and growth opportunities can be expected under policy option 2[169]. As under policy option 2, additional direct and indirect benefits are expected, though could not be quantified.

Efficiency and productivity gains would amount to around 10%, representing **EUR 131.2 billion p.a.** across the data economy. This is considerably lower than the benefit foreseen under policy option 2, because if companies are forced to share data in a wide range of situations under restrictive conditions, they are unlikely to make major investments in data generation, collection and handling[170]. In other words, as policy option 3 obliges to a wider data access under more stringent technical conditions with less possibilities to recuperate investments, data holders would be dis-incentivized to invest in data generation. This policy option would imply an additional compliance burden to some industry sectors.

Data holders (i.e. IoT solution providers, smart machinery manufacturers) would incur higher costs under policy option 3 as compared to policy option 2 as a result of the obligation to set up and maintain the appropriate technical means for data to be accessed. As an example, extrapolating from fitness trackers to the whole IoT market, this would imply, for developing technical solutions such as APIs, one-off costs of EUR 1.6 billion and recurring costs of EUR 354 million[171].

The more invasive nature of the obligations under this option could deter companies from investing in connected products. In addition, data holders, notably manufacturers, would incur costs to meet the technical requirements. Industry associations estimated that this would, on average, lead to a 3% increase in costs compared to the *status quo*[172].

ii) Increasing availability of data for commercial use and innovation between businesses

Model contract terms and general rules for data access are expected to have a similar positive impact in terms of data-driven innovation, consumer surplus and productivity as under policy option 2. The impact of the unfairness test in policy option 3 would be greater than in policy option 2 as it would apply to all terms in data-sharing contracts (both unilaterally imposed and negotiated by the parties). This option would lead to higher legal and operational costs for data holders and would be more restrictive than policy option 2 in terms of freedom of contract. The benefit of policy option 3 in this area

[168] European Commission (2021). European Commission (2022). *Study to support an Impact Assessment on enhancing the use of data in Europe*, prepared by Deloitte (Section 3.3.3.5.2.2, Table 82)
[169] Ibid.
[170] Ibid.
[171] See European Commission (2021). *Study on enhancing the use of data*, prepared by Deloitte (Section 3.3.2.4.2.1, Table 72). See Annex 8, Table 5, for methodology used to obtain these costs.
[172] European Commission (2022). *Support study for Impact Assessment on Sustainable Product Initiative*.

is expected to be **EUR 7.85 billion p.a.**[173]. Estimated costs for companies would be higher than for policy option 2, totalling around **EUR 79 million p.a.**[174].

Table 3 Costs and benefits of measures on B2C and B2B relations

Measures to increase legal certainty Benefits and costs in 2028 (million EUR p.a.)				
	Policy Option 2		**Policy Option 3**	
	Benefit	**Cost**	**Benefit**	**Cost**
Efficiency and productivity gains and costs	196 700	410 (one-off) 88 p.a.	131 200	1 641 (one-off) 354 p.a.
Savings linked to reduced moving costs	68 100	n/a	90 800	n/a
Total	271 000	410 + 88 p.a.	228 200	1 641 + 354 p.a.

Table 4

Measures to improve contractual fairness Benefits and costs (2021-2030) (million EUR p.a.)				
	Policy Option 2		**Policy Option 3**	
	Benefit	**Cost**	**Benefit**	**Cost**
Total	7 402	69	7 851	79

6.2.2. Intervention in B2G data use

The majority of business stakeholders that responded to the online public consultation are not in favour of mandating B2G data use. They argue that voluntary mechanisms are sufficient, and that obligations would unnecessarily increase their costs and prevent the full monetization of data. In contrast, 38% of responding companies and business organisations/ associations considered that action on B2G data sharing for the public interest is needed (section 2.1, problem 3)[175]. Amongst those that support action, one stakeholder commented that *'data sharing requirements introduced at national level have led not only to a fragmentation of the Digital Single Market, but also create complexities and uncertainty for businesses which are called upon to comply with conflicting EU, national and local regulations, with more than often a duplication of similar requests among public authorities.'*

The impact of **policy option 1** depends on businesses' uptake of non-binding measures and recommendations encouraging B2G data access and reuse practices. In the light of recent observations, such voluntary initiatives are unlikely to prevent regulatory fragmentation nor to offer any real improvement over the instruments already used in B2G context.

[173] European Commission (2022, *forthcoming*). *Study on model contract terms and fairness control in data sharing and in cloud contracts and on data access rights*, prepared by ICF (Section 8.3.3, Table 8.13).
[174] Ibid, (Section 8.3.3, Table 8.14 and Table 8.13).
[175] European Commission (2022). *Outcome of the online consultation on the Data Act*.

Policy option 2 would clarify the conditions and procedures under which public sector bodies could request privately held data needed in exceptional situations. A B2G data sharing mechanism increasing the amount of official statistics by even 20% could generate an additional **EUR 4.4 to 12.5 billion GDP p.a.**[176]. As compared to the *status quo*, where B2G data use requests are not streamlined – resulting in time-consuming negotiation processes – businesses could save up to **EUR 155 million p.a.** across the EU due to a lower administrative burden[177]. In addition, non-quantifiable benefits include improved reputation, better analysis methods and models.

The Deloitte study was not restricted to exceptional situations; it focused on currently active B2G partnerships in the five sectors within the scope of the study (supermarkets, commercial banks, telecommunication operators, accommodation platforms, ride-hailing companies)[178]. It is difficult to estimate what proportion of the abovementioned data use requests would be considered as 'exceptional situations' and would therefore fall under this policy option. However, it can be assumed that the benefits and costs mentioned in this section related to B2G, both for policy option 2 and policy option 3, would be partially realised.

Businesses responding to requests would incur costs for the technical solutions to make the data available which depends on many factors, such as the type of infrastructure needed, the format in which data would be delivered and the level of customisation needed. The Deloitte study estimates that policy option 2 could incur one-off costs to businesses up to **EUR 552.5 million** across the EU[179]. In addition, the recurring annual costs to businesses resulting from B2G data sharing would amount up to **EUR 78.1 million** across the EU (identifying, normalising and making data available for reuse)[180]. In practice, the costs are likely to be lower, since most companies that collect and process data are already equipped with the technology, infrastructure and know how to respond to the data requests without incurring sizeable new costs. Moreover, businesses would, except in case of public emergencies, receive compensation for the costs incurred in providing the data plus a reasonable return on investment (RoI) (see section 5.2).

Policy option 3 would entail higher administrative and compliance costs for companies than policy option 2, without necessarily compensating them with greater benefits. The benefits to data holders in terms of the reduced administrative burden is expected to be similar to policy option 2[181].

[176] ESTAT (2021). *Methodological support to impact assessment of using privately held data by official statistics*, prepared by Consulting Gruppe (p. 136).
[177] European Commission (2022). *Study to support an Impact Assessment on enhancing the use of data in Europe*, prepared by Deloitte (Section 3.3.1.4.2.2, Table 64 and Annex 4, Table 5).
[178] European Commission (2022). *Study to support an Impact Assessment on enhancing the use of data in Europe*, prepared by Deloitte.
[179] European Commission (2022). *Study to support an Impact Assessment on enhancing the use of data in Europe*, prepared by Deloitte (Section 3.3.1.4.2).
[180] Ibid.
[181] European Commission (2021). European Commission (2022). *Study to support an Impact Assessment on enhancing the use of data in Europe*, prepared by Deloitte (Section 3.3.1.5.2.1).

Under policy option 3, businesses would incur similar costs to policy option 2, apart from the creation of a data steward function. However, in this option, businesses would only recuperate marginal costs (as compared to a costs plus reasonable return on investments under policy option 2) and would therefore incur higher costs. In addition, the flexibility in defining public interest tasks covered would mean less predictability and harmonisation of requests for EU businesses.

The designation of a data steward is estimated to cost on average **EUR 210 000**. Since all large businesses would have to create such a function, it could cost up to **EUR 68.3 million p.a.** (in the private sector)[182]. While benefits could not be quantified, they include time savings in finding the right contact point within an organisation, knowledge creation and reduced requests for data that is not available. Data stewards would benefit in particular businesses that receive many requests for data.

Table 5

Measures to increase B2G data use Benefits and costs for businesses in 2028 (million EUR p.a.)				
	Policy Option 2*		**Policy Option 3**	
	Benefit	**Cost**	**Benefit**	**Cost**
Economic impact of mechanism on reuse for specific purposes	>4 400**	552.5 (one-off) 78.1 (p.a.)	>4 400**	n/a
Impact on administrative burden (for businesses)	155	n/a	>155	n/a
Designation of data stewards	n/a	n/a	n/a	68.3
Total	>4 555	552.5 + 78.1 p.a.	>4 555	68.3

*The Deloitte study was not restricted to 'exceptional situations'.

**Based on a study done for EUROSTAT: this figure, which relates to GDP growth in 2018-2030, represents the lower end estimate of gains from additional 20% public statistics only. Broader societal and environmental benefits are treated in section 5.3.

6.2.3. Intervention on cloud and edge services

In general, significant positive impacts on businesses are to be expected through the measures related to cloud and edge services. Removing hurdles to cloud switching would enable European businesses to benefit from more innovative and competitive cloud and edge services. This would also give providers (mostly smaller, EU-native providers) the possibility to tap into new market potential as a result of the more competitive market.

Policy option 1 would have a limited impact on businesses, as experience shows that existing non-binding measures related to portability/interoperability, such as the SWIPO codes of conduct, have not produced a balanced realisation of the potential value of data[183]. Under this scenario, the potential impacts of non-binding measures would largely

[182] European Commission (2021). European Commission (2022). *Study to support an Impact Assessment on enhancing the use of data in Europe*, prepared by Deloitte (Section 3.3.1.5.2.1).
[183] SWD(2018) 125 final; OJ L 134, 31.5.2018, p. 12-18.

be dependent on the reaction of the digital industry to the Commission's recommendations to improve the SWIPO codes of conduct.[184] Given the negative track record shown by the industry previously in developing these codes of conduct (in terms of scope of the codes and the significant delays suffered), expectations in this regard must be low.

However, an additional **0.03 percentage points of EU GDP** could be generated, if the industry were to show commitment to improve the codes of conduct and raise more awareness of the initiative[185]. Policy option 1 would not eliminate businesses' concerns of potential unlawful access by third countries.

Under **policy option 2**, cloud switching would be improved in practice through a set of binding framework conditions that would eliminate contractual hurdles inhibiting switching today and largely remove applicable charges.

The most important economic benefits for businesses of the proposed cloud intervention under policy option 2 is that it would pave the way to a modern cloud/edge services offering, which Europe needs in terms of innovation[186]: a seamless, multi-vendor federated cloud space that will lead to a myriad of new data processing functionalities[187]. This would connect well to the strategy of federating data processing capacities scattered across the EU, to support the next-generation of fully interoperable, energy efficient and competitive European cloud-to-edge based services[188]. It would allow businesses, particularly SMEs, to be competitive, commercially viable, scalable in the EU market, and facilitate the deployment of new technologies (such as big data analytics, machine learning and AI tools or IoT operating systems, which require a federated environment of interoperable cloud and edge services as a basis[189]).

Furthermore, the intervention under policy option 2 will benefit users of cloud and edge services by reducing the cost of switching providers, which currently goes up to 125% of annual subscription costs[190]. This assessment would be in line with the reasoning of the EU's largest native cloud provider in favour of this approach: *'Legislation could include high-level principles that would recognize the right for cloud service portability, as well as more specific set of conditions of contractual, technical, commercial and economic nature […]. EU legislation, by letting the industry develop standards and formats […] could contribute to increase the use of interoperable and open formats by the users'*[191].

[184] See section 2.2. of this Impact Assessment.
[185] European Commission (2018). *Switching of cloud services providers*, prepared by IDC and Arthur's Legal, p. 93.
[186] As defined in the European Data Strategy and Digital Decade Policy Programme.
[187] Some cloud providers already offer tools that provide a certain degree of abstraction from the infrastructure used, but such tools only work for simple data storage services.
[188] This is also in line with the work programmes of the Commission's funding instruments: the Connecting Europe Facility 2, Digital Europe Programme, Horizon2020, Recovery and Resilience Facility
[189] 27 leading EU ICT providers (2021). *European industrial technology roadmap for the next generation cloud-edge offering.*
[190] European Commission (2018). *Switching of cloud services providers*, prepared by IDC and Arthur's Legal.
[191] OVHCloud's Position Paper on the Data Act (2021).

In terms of concrete macro-economic impacts, the enforceable legal obligation of switching, accompanied by the new repository for open interoperability standards, should make switching easier and increase the take-up of cloud services in the EU. It is expected to increase cooperation amongst market players and streamline portability solutions on technical and contractual levels. It would generate an additional 10.9% demand for cloud in 2025 (**EUR 7.1 billion**) as compared to no action on this[192]. Due to increased take-up of public cloud, policy option 2 could add **0.05 percentage points to EU GDP**[193].

As regards costs, a regulatory approach to cloud switching could bring increased compliance costs for ***cloud service providers***. However, as the proposed approach under policy option 2 would not include mandatory interoperability requirements but rather builds on an industry-led standardisation approach, the costs are expected to remain manageable, especially where service offerings of providers already contain software features to facilitate export of data. Cloud providers with services based on proprietary standards and without clear processes in place for switching would face more costs, in particular for the redesign of services to comply with the mandatory framework conditions for switching (e.g., to respect timeframes). This will also incentivize software developers to foresee data export features from the beginning in the design of their applications. However, initial costs are expected to be outweighed by the benefits for the providers from additional demand for cloud services[194].

As regards the costs of the intervention to tackle the trustworthiness problem related to third country access to data, the support study for this IA found that leading cloud service providers do not yet implement the full array of legal, technical, and organisational mitigating measures included in policy option 2. Although their offer is being gradually improved in that respect, much more would need to be done to prevent access and transfer requests that would be in conflict with EU law. In other words, this policy option could advance the solutions that would become state of the art in the medium term. This makes it difficult to distinguish the costs of regulatory compliance from the investments of the cloud providers under the baseline scenario. The real advantage of regulation is therefore the time aspect (voluntary changes being slow), the level-playing field for all cloud providers (price competition will not happen at the expense of mitigating measures) and the strengthening of trust in the cloud environment. The latter aspect is particularly important at this juncture for the data economy since stakeholders expressed serious concerns about the current situation. As these investments would advance the state of the art of the cloud industry, the costs for cloud service providers under this option may be considered 'advanced investment'[195].

Some stakeholders in the online consultation warn against deploying a legislative approach to include such mitigating measures as they may invoke reciprocal action by

[192] European Commission (2018). Switching of cloud services providers, prepared by IDC and Arthur's Legal, p. 6.
[193] Ibid, p. 94.
[194] Ibid.
[195] European Commission (2022). *Study to support an Impact Assessment on enhancing the use of data in Europe*, prepared by Deloitte (Section 3.3.4.1.3).

non-EU/EEA authorities. This may lead to a loss in sales of EU services to non-EU clients. Some stakeholders argue that a multilateral approach should be favoured, e.g., in the context of the OECD's work on trusted government access to data[196].

As regards the standardisation repository for cloud and edge interoperability standards presented by policy option 2, this would present no fixed additional costs for businesses, as the approach would depend on voluntary participation in an industry-led standardisation process. Businesses would therefore be able to keep any additional costs under their own control.

Policy option 3 is not expected to produce higher benefits than policy option 2 but would lead to higher costs for industrial actors[197]. These would be mostly the result of the mandatory interoperability requirements, as a result of which businesses would need to restructure their current services to match the required standards, instead of allowing a gradual industry-led standardisation process towards achieving open interoperability standards. Indeed, earlier experiences show that compliance to compulsory standardisation is expensive and time consuming[198].

In addition, mandatory technical elements could stifle innovation by data processing service providers and, in turn, by user industries. Innovation could be affected by lengthier product development cycles, as compliance would have to be built into new service offerings[199]. Also, legally mandated APIs may be inappropriate given the diversity of service types on the market (e.g., infrastructure, platform, and software services) and functionalities (ranging from simple data storage to highly tailored software applications). A given user of cloud services, such as an email client, is likely to use data architecture and semantics quite differently from those used for delivering another service type, like a Customer Relations Management system.

At the same time, it is likely that the direct and general portability obligation as proposed under policy option 3 may be less effective than an approach specifying contractual and/or economic parameters (as under policy option 2). As the example of the portability right of the GDPR shows, a broad and high-level provision may lead to uncertainties for public authorities as regards the applicable modalities and the enforcement/implementation.

Table 6

Measures to facilitate switching between cloud and edge services Benefits and costs for businesses in 2025 (million EUR p.a.)				
	Policy option 2		**Policy option 3**	
	Benefit	**Cost**	**Benefit**	**Cost**
Obligation to allow	7 100	n/a	7 100	n/a

[196] European Commission (2022). *Outcome of the online consultation on the Data Act*.
[197] European Commission (2018). *Switching of cloud services providers*, prepared by IDC and Arthur's Legal.
[198] E.g., COM/2016/0478 final/2.
[199] European Commission (2018). *Switching of cloud services providers*, study prepared by International Data Corporation (IDC) and Arthur's Legal.

switching				
Addressing concerns of unlawful access	n/a	n/a	n/a	n/a
Total	7 100	n/a	7 100	n/a

6.2.4. Intervention to improve data interoperability

The Data Act aims to introduce a mechanism to address data interoperability, which is a precondition for efficient data sharing within and across sectors.

An overwhelming majority (92%) of the respondents to the online consultation on the Data Strategy indicated that standardisation is necessary to improve interoperability and ultimately data reuse across sectors[200]. While standardisation issues are addressed indirectly and only partly by the creation of the European Data Innovation Board under the Data Governance Act proposal, contacts with stakeholders and political discussions (with the European Parliament and Council) show that further action at the European level is expected, given the potential benefits.

The costs of developing standards were estimated in the Impact Assessment of the Standardisation Regulation 1025/2012 at **EUR 1 million** per standard[201].

In **policy option 1**, the impact of non-binding recommendations on the use of specific standards will ultimately depend on their uptake by stakeholders, which as demonstrated throughout this report, would likely be low[202]. Regardless, some data reusers (e.g., businesses, consumers, researchers) will end up saving in costs and time due to the (voluntary) uptake of such data interoperability measures established for some common European data spaces.

Under **policy option 2** if the current standardisation mechanisms (led by industry or a European Standardisation Organisation) do not sufficiently enable cross-sectoral data use, the Commission could, by way of an implementing act, lay down common specifications for interoperability requirements. In this event, businesses would incur costs in order to comply with the resulting binding obligations. At the same time, this harmonisation would reduce transaction costs linked to the (re)formatting needs to transmit and use data across the market.

Under **policy option 3**, the Commission would lay down interoperability requirements in implementing acts to facilitate data use in and across sectors. This would lead to higher costs for businesses than policy option 2, as it would require full compliance with the new requirements. However, a similar reduction in transaction costs can be expected.

6.3. Impact on SMEs

6.3.1. Impacts on SMEs in B2B and B2C contexts

[200] European Commission (2020). *Outcome of the online consultation on the European strategy for data*.
[201] SEC(2011) 671 final, p. 8. According to this Impact Assessment, 'The ESOs point out that this cost is financed primarily by industry (93-95%) followed by national governments (around 3-5%) and the European Commission/EFTA contribution (around 2%).'
[202] See section 2.2. of this Impact Assessment.

About 99% of both data supplier and data user companies in the EU are SMEs. To innovate, they need to acquire more business-critical data from other companies than larger enterprises[203]. However, a 2019 survey indicated that 40% of SMEs struggle to access the data they need to develop data-driven products and services, notably because they lack bargaining power to negotiate with data holders[204].

By re-balancing the distribution of data value across market actors, the Data Act would bring more data resources within reach of SMEs, thereby reinforcing their ability to compete and continue their business[205]. This will concern SMEs both in their capacity of the users of various connected products (e.g., industrial machines), as well as providers of data-based services.

The position papers submitted in the context of the public consultation indicate that a level-playing field for OEMs and other data holders is of particular significance in markets with a high concentration of SMEs and sole traders (e.g. providers of aftermarket and repair services, craftsmen, farmers)[206]. The ICF study found that if the abuse of a considerable negotiating power imbalance in bilateral contractual relations is addressed, SMEs would find it easier to enter the market with new business models. In such cases, fairness in data-sharing agreements could contribute to productivity gains as more data would be available for data-driven innovation and/ or there would be more opportunities to break into the market with new business models[207]. This study shows that under policy options 2 and 3, SMEs would benefit from annual net profits of around EUR 5.2 billion (EUR 17 400 per SME) and EUR 5.5 billion (EUR 18 400 per SME)[208] respectively for this aspect of the initiative. Hence, around 71% of the benefits of all three policy options would accrue to SMEs, and the remaining 29% to large companies.

The Data Act would make it possible for users of connected products to benefit from data-based services provided by companies (in case of aftermarket services – composed overwhelmingly of SMEs[209]) other than the manufacturer or original service provider.

The lack of a clear legal framework means SMEs suffer disproportionately more than large companies as they cannot afford the necessary legal advice to draft and negotiate contracts[210]. As such, clearer rules on data rights along with fairer data contracts will benefit SMEs proportionally more. The use of model contract terms is therefore expected to make a significant contribution to increased data sharing. As shown in section 6.2, they are supported by a large majority of the respondents to the public consultation and, in particular, by micro companies and SMEs.

---

[203] Bianchini, M. and V. Michalkova (2019). *Data Analytics in SMEs: trends and policies*, OECD SME and Entrepreneurship Papers, No. 15, OECD Publishing, Paris.
[204] European Commission (2019). *SME panel consultation B2B data sharing - Final Report*.
[205] SMEunited's position paper on Access to Data.
[206] SMEunited's position paper on Access to Data.
[207] European Commission (2022, *forthcoming*). *Study on model contract terms and fairness control in data sharing and in cloud contracts and on data access rights*, prepared by ICF (Section 8.2.2).
[208] Ibid (Section 8.3.1.3, Table 8.14).
[209] E.g. In markets for vehicle parts, diagnostics, servicing and repair of vehicles.
[210] SMEunited's position paper on Access to Data. The same was explained by SMEs participating in a workshop organised by the European Commission on the Data Act, on 7 July 2021.

Regulatory adaptation costs for SMEs (as data users) will be low in comparison to the expected high benefits due to wider data reuse, cross-selling, and the possibility to offer added-value services. Nevertheless, many SMEs consulted who are also data holders expressed fears of becoming 'data donors to large tech companies'. Combining the model contract terms with the unfairness test will mitigate this risk by the possibility under policy option 2 for data holders to modulate/adapt the terms for data access according to the size and role of the business entity in the value chain, including via sectoral legislation.

6.3.2. Impacts on SMEs in B2G contexts

SMEs would benefit directly from a more efficient and robust public service (e.g., more granular and accurate market statistics) or indirectly (thanks to the positive impact of B2G on GDP). To alleviate the potential burden of certain actors to comply with data access request, small and micro companies would be in principle exempt of this obligation in policy option 2.

6.3.3. Impacts on SMEs of cloud related measures

SMEs and start-ups would be the greatest beneficiaries from an intervention on cloud switching, as users of cloud and edge services but also as providers of such services.

On the demand side, regulatory intervention to facilitate cloud switching would mostly benefit high-tech SMEs and start-ups that use cloud and edge services due to the harmonised market conditions across the EU[211]. Larger organisations may be better equipped to handle technical problems related to a lack of standardisation (e.g., application portability), but SMEs are not[212]. In addition, SMEs lack the resources to re-architecture their digital assets in order to move them to new platforms, which is necessary as proprietary standards are still often used by actors on the market.

On the supply side, the smaller, often EU-native providers of cloud and edge services will benefit most from the proposed intervention on cloud switching. Firstly, the smaller providers have most to gain and least to lose in terms of customer base. Whereas currently their potential customers are locked into the integrated ecosystems of larger providers with proprietary standards, a legislative approach to foster cloud switching will unlock this very large customer potential[213]. Ease of switching is often a commercial argument put forward by (smaller) European providers, to distinguish themselves from hyperscalers[214]. Secondly, the most important benefit for smaller cloud and edge providers is to be expected from the development of open standards and interfaces through the new standardisation approach in policy option 2, which would allow the smaller providers to technically build their services around the publicly available open

[211] European Commission (2018). *Switching of cloud services providers*, prepared by IDC and Arthur's Legal, p. 91
[212] Ibid, p. 4, 5.
[213] N. Kratzke & P. Quint (2018), Project CloudTRANSIT: Transfer cloud-native applications at runtime, see *here.*
[214] OVHCloud, ibid

standards and interfaces without having to bear the costs to develop those. New open standards presented in a repository will offer SME providers the certainty that their services can connect to customers and other relevant cloud services. Thirdly, policy option 2 would support new and existing partnership initiatives of European smaller providers in the area of cloud federation, in order to increase the scalability of European cloud and edge providers by allowing users to resort to multiple cloud or edge functionalities of different providers, and to decrease the dependency on non-EU/EEA providers.[215] This explains also why smaller European providers have called for a regulatory intervention on cloud switching in the Data Act, and are not asking for any exception of themselves in this regard. A small European cloud provider stated '*After the lack of impact of the SWIPO codes of conduct, developing a new kind of self-voluntary approach (…) will only be a way to preserve the status quo. We need hard law, at EU level, to progress towards greater data portability*'[216].

Further than problems related to vendor lock-in, SMEs are also confronted with problems of generally unbalanced contracts with cloud providers, which generated a gross economic detriment equal to EUR 653 million over a 2-year period. Reducing distrust in cloud and increasing competition is expected to reduce the abovementioned losses and to rebalance the uptake of cloud services between large and small companies[217].

6.3.4. Impacts on SMEs in the context of data interoperability

SMEs will benefit from improved interoperability across sectors, facilitating the use of data for these actors. Transaction costs relating to the curating, formatting or annotation of data are reduced and with that enable the analysis of data and ease the combination with other relevant sources.

6.4. Impact on consumers

The Data Act would benefit citizens both directly, in their capacity of consumers, and indirectly, as beneficiaries of public services (on the latter, see section 6.5.).

As regards B2B and B2C, in **policy option 1**, a voluntary scheme to access data from the use of products or services in order to move to alternative services might benefit consumers in certain sectors but as mentioned in section 6.2., the impact of this policy option is likely to be low. Consumers would be amongst the main beneficiaries of **policy options 2 and 3** as they use an increasing array of connected products, such as fitness trackers, smart home devices, mobility devices. Consumers would benefit from being able to access the data generated thanks to their use of such connected products in the following ways: (1) increased consumer choice and mitigation of 'lock-in' to particular connected products and related services; (2) ability to repair connected products and reduce unnecessary waste; (3) incentives to develop new or improved services and

[215] Centrum für Europäische Politik (2020), *European leadership in the digital economy*, p. 115, see *here.*
[216] Scaleway (2021). *Full steam ahead towards a true multi-cloud offering to deliver on broken promises*.
[217] European Commission (2018). *Study on the economic detriment to small and medium-sized enterprises arising from unfair and unbalanced cloud computing contracts*, prepared by EY.

products for customers; and (4) more efficient connected products in terms of energy consumption and functionalities offered.

However, the impact of the benefits for consumers described above would be lower under policy option 3 than policy option 2 because of the disincentives for data holders to invest in data generation (see section 6.2.1.).

An unfairness test, while encouraging more data sharing, may also contribute to increased competition in terms of price and differentiation, which would result in increased consumer surplus. There are similar practices already taking place in certain contexts. For example, in the aviation sector, Rolls-Royce is already making repair data available as a result of action from their industry. This shows that a company can lose bargaining power over their data but at the same time become more competitive in their market of relevant products and services[218].

6.5. Impact on public administrations

Public administrations are likely to be impacted mostly by the measures intended to enhance B2G data sharing. The public sector will gain new ways to access data to tackle societal and environmental problems of exceptional nature. This will increase the efficiency of public services, with a positive spill-over effect across the whole economy (e.g., thanks to more reliable statistical information), benefitting the public sector once again (e.g., via positive impact on GDP and related higher budget income).

Under **policy option 1**, any improvement in terms of enhanced access to or the reuse of business data is unlikely unless Member States chose to implement the Commission's recommendations, and there would be no legal basis for EU bodies to reuse such data[219]. Governmental revenues[220] would not be impacted significantly[221].

Policy option 2 would lead to an annual increase in governmental revenues of up to **EUR 96.8 billion in 2028**, which is more than the other policy options[222]. As regards B2G, public sector bodies would have access to more data in an easier and timelier manner in exceptional situations (including public emergencies), leading to more effective spending. For example, in the context of the COVID-19 pandemic, mobility data is being used to inform decisions on local lockdown measures, which helps reduce losses[223]. Overall, the Deloitte support study showed that B2G efficiency gains could lead to savings of up to **EUR 337 million p.a.** for national and local authorities across the

[218] European Commission (2022, *forthcoming*). *Study on model contract terms and fairness control in data sharing and in cloud contracts and on data access rights*, prepared by ICF (Section 8.2.4).
[219] European Commission (2022). *Study to support an Impact Assessment on enhancing the use of data in Europe*, prepared by Deloitte (Section 3.4.1.1).
[220] According to the definition of Eurostat, the governmental revenue is the sum market output, of taxes, net social contributions, sales, other current revenues and capital transfer revenues. See Eurostat 2020, *Statistics Explained, Glossary: government revenue and expenditure*, available *here*.
[221] European Commission (2022). *Study to support an Impact Assessment on enhancing the use of data in Europe*, prepared by Deloitte (Section 2.5.3.1.3).
[222] Ibid.
[223] ESTAT (2021). *Methodological support to impact assessment of using privately held data by official statistics*, prepared by Consulting Gruppe.

EU[224]. In addition, up to EUR 64.8 million of costs could be reduced for statistical offices across the EU in view of access to companies' data just for the calculation of the Consumer Price Index[225]. However, as mentioned in section 6.2., these figures are not limited to exceptional situations, so the actual savings would likely be lower.

The total cost to public sector bodies across the EU for ensuring national structures under policy option 2 could amount to **EUR 21.6 million p.a.**[226].

In addition, Member States would face reasonably low additional costs associated with the enforcement of the Data Act's cloud provisions, which would be awarded to existing national regulatory authorities. As it can be expected that the number of complaints about switching received at national level will be low, around 2 or 3 p.a., the additional human resources cost is estimated to be EUR **585 000** for all Member States combined, and roughly EUR **50 000** for the European Commission (see Annex 4).

In **policy option 3**, Member States would benefit from the flexibility of being able to request data beyond exceptional situations, for any duly justified purpose, at marginal cost. As a consequence, benefits are likely to be higher than for policy option 2 due to a wider range of data in scope, but the support studies have been unable to quantify this due to the flexibility of policy option 3. This option would lead to an annual increase in governmental revenues of up to **EUR 34.6 billion in 2028**[227].

Costs for public sector bodies would be similar to those incurred under policy option 2. In addition, the creation of a data steward function (obligatory under policy option 3) would cost around **EUR 314.8 million p.a.**[228] in the public sector.

Table 7

Measures to increase B2G data use Benefits and costs for public administrations in 2028 (million EUR p.a.)				
	Policy option 2*		**Policy option 3**	
	Benefit	**Cost**	**Benefit**	**Cost**
Efficiency of national structures	337	21.6	>337	21.6
Designation of data stewards	n/a	n/a	n/a	314.8
Total	337	21.6	>337	336.4

* The Deloitte study was not restricted to 'exceptional situations'. Please see explanation in section 6.2 (B2G, PO2) above.

[224] European Commission (2022). *Study to support an Impact Assessment on enhancing the use of data in Europe*, prepared by Deloitte (Section 3.3.1.4.2).
[225] European Commission (2022). *Study to support an Impact Assessment on enhancing the use of data in Europe*, prepared by Deloitte (Section 3.3.1.4.2).
[226] Ibid (Section 3.3.1.5.2.1, Table 66).
[227] Ibid (Section 2.5.3.1.3, Figure 23).
[228] European Commission (2022). *Study to support an Impact Assessment on enhancing the use of data in Europe*, prepared by Deloitte (Section 3.3.1.5.2.1).

6.6. Social and environmental impact

Social and environmental benefits are expected due to increased efficiency in tackling societal challenges and using data to contribute to the Green Deal. However, enhancing data sharing and access may also be associated with certain risks (see Annex 8).

Policy option 1

The impact under policy option 1 is contingent upon uptake by stakeholders, in particular Member States. However, their reticence to follow the 2018 data-sharing principles (see section 2.1.) makes such uptake improbable. Possible positive impacts in terms of consumer empowerment, process efficiency with knock-on effects on environment, better policymaking, etc. might be expected, but to a minimal degree given that they would be driven by the most committed actors only (e.g. as part of their CSR activities).

Policy option 2

Policy option 2 includes measures on B2G data sharing that would increase the quality and quantity of data available to public sector bodies, in particular to respond rapidly and effectively to public emergencies. The limited focus on exceptional situations would minimise any undue burden on businesses and it would address the concern expressed by some stakeholders in the private sector that B2G data sharing must always be legitimate.

Social impacts

In terms of **social impacts,** based on stakeholders' estimates, B2G could reduce costs for public sector bodies by up to 1% due to increased efficiency in tackling societal challenges[229]. For example, the annual contribution of B2G data sharing in 2030 in the area of health (in terms of public health and R&D on health) could be significant. According to a recent study for the period 2018-2030, this could overall add between **EUR 76 to 109 billion to GDP**[230] through the benefits of better data use. While under this policy option B2G use is limited to exceptional situations, given the magnitude of these figures, it can be assumed that the benefits would still be substantial.

In the B2C context, the empowerment of consumers with regard to the use of the data they generate is likely to enhance their active participation in the digital economy, contributing to digital awareness and helping reduce the digital divide. Better availability of data should also stimulate research (both private – in the B2B context – and public – in the B2G context). In addition, the enhanced innovation and competition would benefit employment levels (quantified in the preceding chapter), with all ensuing effects in terms of social inclusion, better access to education and healthcare, etc.

Environmental impacts

[229] Ibid, (Section 3.3.1.4.2).

[230] Calculation based on share of government expenditure on general public services as part of national accounts statistics (see *here*), following the methodology developed in ESTAT (2021). *Methodological support to impact assessment of using privately held data by official statistics*, prepared by Consulting Gruppe.

As for the **environmental impact**, B2G data use in the area of environmental protection (in terms of pollution abatement, biodiversity protection and R&D related to environmental protection) could, according to estimates by EUROSTAT for the period 2018-2030, add between **EUR 65 to 93 billion to GDP**[231] through the benefits of better data use. Again, even though this policy option is limited to exceptional situations, it can be assumed that the actual benefits would still be substantial.

For example, access to and use by public sector bodies of direct economic loss data, including the costs of emergency response and recovery, could improve the accuracy of the risk assessments that inform climate adaptation actions. Policy option 2 could also enable businesses and consumers to use data more efficiently and encourage innovation contributing to Green Deal objectives, including improved energy efficiency, increased share of renewables and reduced greenhouse gas emissions[232]. Increased reparability and optimization opportunities, due to better data access in the context of predictive maintenance services carried out by independent repairers, should translate into a longer usage time for connected products[233]. Allowing consumers to access data from their products and have it analysed by a service provider of their choice could inform their decisions about the category of device to purchase. They would be in a better position to choose a device that suits their needs, for example using a less powerful device for browsing the web and making video calls could lead to significant energy savings. Data from insurers on damage to buildings, infrastructure and agriculture can help decision-makers take informed decisions to improve resilience and adaptation capacity[234].

In infrastructure and transport research, newly available data could improve citizens' living and working conditions while contributing to environmentally friendly urban development[235]. Providing emissions data for logistics has enabled a footwear retailer to make more efficient shipments, reducing CO_2 emissions by 48%[236].

In construction, analytical tools are capable of converting sensor data into actionable information about the source of failures (e.g. related to insulation and vapour barriers).

[231] ESTAT (2021). *Methodological support to impact assessment of using privately held data by official statistics*, prepared by Consulting Gruppe.
[232] IEA (2019), *Energy efficiency and digitalisation*, IEA, Paris; American Council for an Energy Efficient Economy (2020). *Intelligent efficiency*; Ben Youssef, A. (2020). *How can industry 4.0 contribute to combatting climate change?* Revue d'économie industrielle, No. 169; Garetti, M. and Taisch, M. (2012). *Sustainable manufacturing: trends and research challenges*, Production Planning and Control, No. 23.
[233] European Commission (2022). *Study to support an Impact Assessment on enhancing the use of data in Europe*, prepared by Deloitte (Section 3.3.3.4.2.2).
[234] European Commission (2022). *Study to support an Impact Assessment on enhancing the use of data in Europe*, prepared by Deloitte (Section 3.3.1.4.2.2).
[235] For instance, the 'Transforming Transport' project, part of the Horizon 2020 strategy, shows that the use of Big Data in transport in logistics could contribute to an important saving in fuel and 380 megatons of CO2 emissions in addition to saving time for citizens. Yet only 19% of EU mobility and logistics adopt Big Data solutions.
[236] SWD(2020) 331 final.

This could reduce the over 800 million tonnes of construction and demolition waste generated per year in Europe[237].

The introduction of binding rules to facilitate cloud switching, especially when accompanied by interoperability standards, would force companies to improve the interoperability of their systems. With a minimum level of interoperability ensured, migration processes would need less processing power and thus have less of an environmental impact.

Policy option 3

Social impacts

In addition to the social impacts identified under policy option 2, policy option 3 provides for a wider range of potential actors in the B2B context and a wider scope of applicability of the B2G provisions. This is expected to lead to substantial social benefits, although the support studies were unable to quantify these benefits. At the same time, policy option 3 would massively increase the access to data for users and is expected to make data-holder companies less willing to invest in connected products. In the B2G context, concerns have been expressed that a widespread use of company data by public sector bodies could lead to undesirable surveillance practices.

Environmental impacts

In addition to the environmental benefits indicated under policy option 2, this option would make the environmental impact of products clearer for businesses along supply chains in all sectors. The supplementary benefits could be substantial. Stakeholders estimate that this could reduce the comparative market share of those products that have an environmental impact and yield a 75% cost reduction for maintenance and repair, a doubling of repair rates and a 20% increase in lifetime of durable goods and hence reduction in the environmental impact of these durable goods by 20%[238]. Moreover, the sharing of logistics data would help reduce traffic congestion and increase the number of parcel deliveries at each vehicle stop. It would also allow the environmental footprint of urban deliveries to be measured and reduced[239].

7. HOW DO THE OPTIONS COMPARE?

PO1 – Non-binding measures encouraging wider and more efficient data access, use and processing among stakeholders	PO2 - Rules on controlled and predictable data access and use	PO3 – Rules for open data access between businesses and from businesses to public bodies

[237] Deloitte (2017). *Study on resource efficient use of mixed wastes, improving management of construction and demolition waste – Final Report*, prepared for DG ENV; Eionet Report (2020). *Construction and Demolition Waste: challenges and opportunities in a circular economy*.
[238] European Commission (2022). *Study report supporting Impact Assessment accompanying the Sustainable Product Initiative*.
[239] European Commission (2020). *Towards a European strategy on business-to-government data sharing for the public interest*, Final Report of the High-Level Expert Group on B2G Data Sharing.

Efficiency (expected benefits, cost effectiveness)		
This option is cost effective: as a voluntary engagement, only the companies that have a clear business interest in adhering to the non-binding guidance will do so. In B2B/B2C context, the promotion of model contracts is the only element of the policy option where tangible benefits are expected (over 5 billion euros p.a.). Similarly, voluntary commitment to improve the fairness of cloud and edge services is also likely to have a (slight) positive impact on GDP growth. In B2G relationships, the low uptake of existing recommendations and principles makes the achievement of the (theoretically substantial) socio-economic benefits illusory. Overall, the limited uptake of non-binding measures (likely to be applied by a subset of companies only) means that the expected macro-economic benefits will be significantly smaller in comparison to those brought about by the binding measures in PO2 and PO3. This implies only a slight improvement over the baseline scenario.	The measures under PO2 that tackle legal uncertainty and empower users should induce a higher availability of data for device users and businesses (mostly SMEs). This new source of data in the market will both spur the creation of new services (by actors who currently cannot access such data easily) and enhance competition in the aftermarkets, ensuring a more efficient resource allocation. These benefits are similar to what can be expected under PO3 and substantially higher in comparison to PO1. Costs of this policy option would fall mostly on data holders (e.g. manufacturers) and cloud providers. They would be more limited than in PO3 (unfairness test narrower, technical means for data access not mandatory) and may outweigh the benefits in the early stages of implementation, but benefit/ cost ratio will be positive in the longer run. Adjustment costs of this option would be much higher than those under PO1 (in terms of technical means of ensuring access to data, changing of current business models) as they would concern all companies in scope, not only those willing to make such investments. At the same time, the 'light touch' approach to cloud switching and data standardisation (in comparison to the more prescriptive measures in PO3) are likely to lead to reductions in data processing costs for cloud service users while keeping the service providers' costs at acceptable levels. Under B2G rules, public sector would benefit from wider and more timely data access than can be ensured via voluntary mechanisms (as in PO1) while harmonization with regard to the grounds for B2G requests and fair compensation would reduce the administrative costs for data holders (in particular small and micro companies would be exempt unless the request demonstrates the necessity and proportionality of the request for data from such companies, unlike under PO3). While the related costs	This option presents similar benefits to those induced by PO2 in the B2B and B2C context. It is however characterized by higher administrative and compliance burden on data producers/ holders than under PO2 (binding not only with regard to the aims but also to the means of data access by users and third parties). In comparison to PO1 and PO2, it would also expose data holders to more competition from services based on the data they hold and accordingly, diminish their incentives to invest in data collection. Compliance with compulsory cloud switching and data interoperability standardisation might lead to efficiencies in comparison to PO2 (benefits for cloud users would materialize faster) but will also be more expensive and time consuming for all businesses obliged to adopt the new standards. In B2G area, the option should benefit the public sector to a higher extent than in PO2 (notably due to lower data acquisition costs) but this is offset by a higher administrative burden of the private and public sector (e.g., data steward function) and by higher costs linked to low stakeholder acceptance (e.g., possible complaints). Overall, the evidence as to tangible improvement over PO2 in B2G area is lacking.

	for companies would no doubt exceed those under voluntary sharing (PO1), they will be eclipsed by the resulting social and environmental benefits.	
Effectiveness (the extent to which the PO is likely to achieve the set objectives)		
The effectiveness of a voluntary approach is seriously limited due to its inability to tackle obstacles of a legislative nature (e.g., *sui generis* right), to address the problems for which the lack of stakeholder consensus prevents coordinated action (B2B, B2G, cloud), or to address the possible future fragmentation of the EU market. E.g., within the B2G setting, both data holders and public authorities confirmed[240] that a voluntary data-sharing model would never scale up without legislative push. In addition, interoperability standardisation which is left predominantly to the market might lead to large companies asserting their dominance and "hijacking" the standardisation process and its outcome. In essence, contrary to PO2 and PO3, PO1 is expected to be conducive to reaching the policy objectives only in sectors which are already digitally very mature and for which the adaptation effort would be minimal (and, therefore, close to the baseline scenario).	For B2B and B2C areas, this option is much more likely to attain the specific objectives in comparison to PO1. The adoption of a legally binding instrument that increases legal certainty, introduces the unfairness test along with model contractual terms and lays down general access rules benefiting both device users and aftermarkets, while also providing technical and legal safeguards against misappropriation for data holders, will increase trust among stakeholders, shift control towards data users and boost overall data availability. PO2 is well-suited to reach the objective in B2G context. Binding rules on how and when privately held data can be used by the public sector will become a tool that can be used in addition to the methods currently deployed for that purpose (including voluntary sharing schemes promoted under PO1). PO2 ensures a greater level of cloud switchability through minimum regulatory requirements, as compared to the situation based on voluntary collaboration of stakeholders. At the same time, it stops short of enforcing strong standardization contemplated in PO3 while facilitating the adoption of a minimal set of commonly agreed cross-sector and cross-border interoperability requirements.	When considered against the criterion of effectiveness on its own (without factoring in the impact of a worse benefit/cost ratio), this policy option should be at least as effective in achieving the objectives as PO2 in B2B/B2C context. It would considerably limit the abuse of contractual imbalances, increase the supply of usable data along the value chains and enhance the legal certainty of market participants. It would also minimize the technical obstacles to data sharing which might make it harder for device users to exercise their rights to data in practice (via more emphasis on technical requirements). The option should also be very efficient in ensuring a faster, cheaper, and more harmonized (in comparison to PO2) access to a variety of private sector data for public interest purposes. Finally, PO3 would be more effective than PO2 in terms of facilitating switching while maintaining full-service functionality.
Coherence (alignment with other policy initiatives and instruments)		
Intervention based on non-binding guidance, promotion of model contracts or self-regulation by the stakeholders is very unlikely to endanger the coherence of the legal and policy framework. It can be	The Data Act under this policy option takes fully into account the current legal framework (e.g., GDPR, Database Directive, Trade Secrets Directive, Digital Markets Act, competition law) and does not intend to modify it in any way.	PO3 would also be designed to remain coherent with the existing and evolving legal framework, based on the same principles as PO2. At the same time, greater interference in contractual freedom in comparison with PO2 could be

[240] European Commission (2022). *Study to support an Impact Assessment on enhancing the use of data in Europe*, prepared by Deloitte (Section 3.3.1.3.2).

therefore considered to be well-aligned with the overall policy setting by definition.	Coherence of the Act with future sectoral legislation would be ensured by limiting the scope of the Data Act to problems that are of cross-sectoral nature and allowing for adoption of complementary rules to address sector-specific needs (including the range of data in scope, specific modalities of data transmission or cybersecurity concerns).	expected, leading to more disputes (as the unfairness test would apply to all contractual terms, including those negotiated by the parties) and slightly affecting the overall coherence.
Feasibility (degree of stakeholder support for legislative adoption and/or implementation)		
Non-binding measures are fully feasible and enjoy strong support among the stakeholders. In the public online consultation, the vast majority of business associations and trade bodies (even those representing start-ups and SMEs) presented a very cautious approach, arguing in favour of non-binding measures.	While not as easily implementable as in the case of PO1, the nuanced stakeholder feedback and political encouragement by the MS (e.g., Council conclusions showing general support to more B2B data sharing, first national initiatives on B2G, or the fact that a B2B unfairness rules already exists in a slight majority of the MS) suggest that this option is feasible. Among the companies however, the support to legislative intervention is clearly split depending on the role within the data value chains (device manufacturers largely against, aftermarket players strongly in favour). For B2G, PO2 appears to be easier to accept for the main stakeholders (in comparison to PO3), in particular due to its complementary (in relation to existing mechanisms) and ad-hoc application, thus limiting any associated costs. Interoperability measures within this option should also be feasible to implement, given the approach that prioritizes stakeholder consensus before legislative action.	PO3 is likely to lead to more feasibility issues than PO2. Stronger opposition can be expected from the data holders (this is related to the high costs of this option as discussed under the efficiency criterion). Businesses are likely to see this option as too prescriptive on technical solutions and too intrusive on contractual freedom. Such resistance would likely depend on the specificities and different levels of digitalisation and maturity across sectors. For B2G, more stringent rules and less advantageous compensation mechanisms may reduce the acceptance by companies to comply with data access requests.
Proportionality (matching intensity of policy intervention to the size and nature of the identified problem)		
Reliance on stakeholders' take up of voluntary measures is not proportional given the extent of the problems and the high socio-economic risk of non-action. Policy intervention that is severely limited by its low efficiency cannot offer a proportional solution.	The proposed measures under PO2 would offer a balanced approach, both enlarging the range of parties entitled to access and use of data, while also ensuring the maintenance of control by manufacturers and data holders. Similarly, the measures to enhance cloud switchability aim to fulfil the objectives in a step-by-step manner, minimising the unnecessary burden for service providers. Finally, the approach towards common specifications takes the form of a tool of 'last resort' that would only	PO3 appears overall proportionate when compared to the seriousness of the problems identified. However, higher compliance burden (with respect to PO2) is not justified by a radically better efficiency of this option. This is particularly the case with respect to the requirements placed on data holders in less digitally mature sectors in B2B and B2C scenarios. Intervention based on PO3 would therefore be less proportional with regard to that based on PO2.

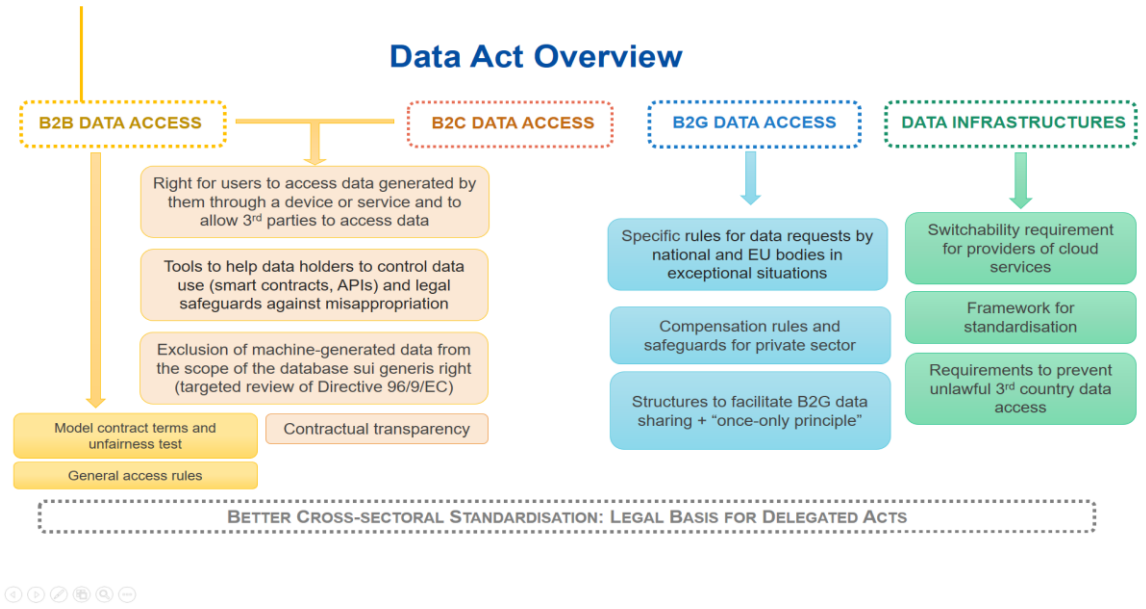
	be activated when the stakeholders are unable to solve the interoperability problems on their own. At the same time, the different elements of this policy option offer a credible solution as to the change in the status quo. Overall, this option appears to be best aligned with the proportionality criterion.	

	Efficiency	Effectiveness	Coherence	Legal/ political feasibility	Proportionality
PO1	**0**	**0**	++	++	-
PO2	++	+	++	+	+
PO3	+	++	+	--	-

The scores reflect the expected magnitude of impact against the baseline scenario: (++) being strongly positive, (+) positive, (0) inducing no noticeable change, and (–) being negative.

8. PREFERRED OPTION

Based on the evidence above, policy option 2 would be the preferred option. The key measures envisaged under policy option 2 are described in Chapter 5. The figure below presents a schematic overview of the policy option.



This package of measures would significantly contribute to increasing the value of the data economy as well as ensuring that data works for society and that a sufficient volume of data is available for reuse, while at the same time providing control mechanisms to maintain incentives to generate data. This would provide for a balanced and feasible approach that is in line with the views expressed by stakeholders, who generally confirm the existence of obstacles to data access and use, while remaining cautious as to the extent and intensity of regulatory intervention in B2B, B2C and B2G settings. In addition, policy option 2 would introduce a legislative approach to the problems of barriers to switching of cloud and edge services and risks of unlawful third country

access to data, but by means of a set of minimum framework conditions for cloud switching. This is the preferred option because, as the experience with the portability right of the GDPR[241] shows, the introduction of a direct but broad portability obligation can lead to differences in interpretation and may provide insufficient guidance for practical interpretation. Finally, the substantially higher costs borne by the data holders under option 3 result in lower political feasibility (i.e. stakeholder resistance).

While a combination of measures from PO 2 and 3 could in theory be contemplated, this would run counter to the adopted approach for setting the level of intensity between the policy options, which is related to the degree of control over the data by the data holder or, from a different perspective to the degree of empowerment of data users.

This logic has been applied to all elements of the policy options in B2B/B2C/B2G areas, in line with the expectations of the stakeholders. It thus affects simultaneously: the range of data in scope, the range of beneficiaries in scope, the technical means of accessing data, the necessary degree of interoperability, etc. This approach facilitated feedback in the consultation phase and was also used by the support studies.

The remaining two intervention areas, focusing on data processing infrastructures and interoperability, follow a different logic in defining the degree of intensity, due to a different set up of stakeholders affected and a different set of underlying problem drivers.

As for the relation with the possible sectoral legislation, the Data Act would follow the approach already applied and tested in the context of the NIS Directive and consisting of a common horizontal framework on which sector-specific legislation can build. The Data Act would leave room for vertical legislation to set more detailed rules addressing sector-specific technical aspects of data access, for example cyber-security, data formats or covering issues going beyond data access as such.

The Data Act will therefore apply to a wide range of data access situations. However, a distinction needs to be made between two scenarios in which the provisions of the Data Act would apply to a varying level of intensity.

Firstly, it will put in place new data access and portability rights for the users of physical products connected via a publicly available electronic communications service and including physical components such as sensors that generate data. Such products may include vehicles, smart home equipment, medical and health devices or agricultural and industrial machinery. Those rights will also extend to data from services functionally linked to those products. This approach ensures that the original data holders (e.g. manufactures of data collecting devices) cannot continue to enjoy a ‘de facto’ exclusivity over the data at the expense of users and other companies, as is currently the case. Such data access rights would however not cover self-standing online services (including banking, insurance, food delivery, platforms providing daily services), beyond those related to products, i.e. in the environment of the Internet of Things. This is because there is no guarantee that access rights to data of all online services would lead to the same

[241] General Data Protection Regulation, Article 20

benefits as in the IoT context. The market structure of IoT suggests that the manufacturers hold an exclusive position over the data that is necessary for aftermarket services. This may not be true with regard to other online services. While some examples of exclusive data use of online services exist and thus access rights in certain sectors are provided for (e.g. banking), there is no compelling evidence to extend new data access rights to all digital services.

Secondly, although only in the context of B2B relationship, the Data Act would lay down general rules on conditions and compensation that should be adhered to all cases (including online services) where a data holder is obliged by law to make data available to another enterprise. This approach should ensure consistently and legal certainty for businesses across the Internal Market. The general principles of the Data Act would apply where the data holder is required to make data available to a third party at the request of the user, and where future instruments are adopted governing business to business data sharing in specific sectors. Likewise, the unfairness test would apply to all data-related contracts unilaterally imposed on micro, small or medium-sized enterprises, across all economic sectors and in all data sharing scenarios.

8.1. Estimated impact of the preferred option

Under policy option 2, EU-27 GDP is expected to **increase from the baseline of EUR 13.80 trillion in 2028 to EUR 14.07 trillion** (equivalent to an additional 1.98% points)[242]. It could lead to EUR 96.8 billion in supplementary government revenues in the period 2024-2028 and EUR 30.4 billion in supplementary investment activities[243]. In addition, policy option 2 could create an additional 2.2 million jobs by 2028[244].

The estimated benefits for the individual policy objectives are as follows[245]:

- Empowering consumers and companies using connected products and related services and increasing the availability of data for commercial use and innovation between businesses would generate up to EUR 196.7 billion p.a. by 2028;
- Improving contractual fairness would bring additional EUR 7.4 billion p.a.;
- Facilitating the use of commercially held data for public interest purposes: reduced administrative burden of up to EUR 155 million p.a.;
- Facilitating access to fair and trustworthy cloud and edge services: additional EUR 7.1 billion p.a.

Costs estimated for the chosen policy option include:

- Obligation of manufacturers to allow access in the B2B/B2C context: EUR 410 million in one-off costs and EUR 88 million in recurrent costs.

[242] European Commission (2022). *Study to support an Impact Assessment on enhancing the use of data in Europe*, prepared by Deloitte (Section 3.5.2).
[243] Ibid (Section 3.5.2.1.2, Figure 40 and Section 3.5.2.1.3, Figure 41).
[244] Ibid (Section 3.5.2.1.1, Figure 39).
[245] See Chapter 6 for the references to the figures provided in this paragraph.

- Ensuring contractual fairness: EUR 69 million p.a.
- B2G data sharing: EUR 552.5 million in one-off costs and EUR 78.1 million in recurrent costs.
- Interoperability requirements: EUR 1 million (per standard).

Overall, given these figures and in view of the reasonable assumptions made to calculate them, it is clear that the benefits far outweigh the costs.

Annexes 7 and 11 describe in more detail how, in practice, the Data Act would resolve issues related to data access and use in a number of practical situations. Annex 7 focuses on B2B, B2C and B2G contexts, whereas Annex 11 focuses on contractual relations.

8.2. REFIT (simplification and improved efficiency)

By clarifying that the *sui generis* right does not apply to databases containing machine-generated data, the targeted review of the Database Directive will also ensure that the Directive will not become an obstacle to sharing such data across sectors. The review will have a positive impact on the uniform application of rules in the EU Single Market and for the data economy.

Quantitative estimates could not be established as there is little awareness amongst industry stakeholders, who may collect and use machine-generated data, of the instrument and its potential use. However, the chosen option is the most effective and coherent as compared to the baseline. This is particularly true considering the increasing volume of data created, shared, and used in the data economy, and the increasing number of situations where the proposed intervention regarding the application of the *sui generis* right to machine-generated data would lead to decreased costs for affected stakeholders as compared to the baseline scenario.

For costs savings beyond those directly linked to the review of the Database Directive, the table below outlines the expectations with regard to the different data sharing scenarios. By intensifying and facilitating data exchanges and use, the Data Act should reduce burden mainly as a result of lowering of the transaction and by inducing costs efficiency gains, both in the public sector and among businesses.

REFIT Cost Savings for the Database Directive[246] – Preferred Option(s)		
Description	***Amount***	***Comments***
Clarifying the application In clarifying that the *sui generis* right does not apply to databases containing machine-generated data, database owners and particularly users would gain certainty that databases containing machine-generated data are not protected by the database right. This intervention would happen at an early stage when the economy-wide IoT rollout is still only nascent. It would prevent that in future, with the expected growth of the sensor-based data economy, the database right becomes a tool to prevent access to data - in contrast to the	Quantitative estimates cannot be established but increase in revenues can be substantial in view of the expansion of data created and shared in the data economy.	Affected stakeholders: Database users

[246] This is the only existing legal instrument changed by the legislation.

other measures proposed in the Data Act. This is expected to facilitate the use of machine-generated data.		
Exclusion of machine-generated data indirectly contributing to increased revenues in data supply chain due to facilitated data sharing. By clarifying that the *sui generis* right does not apply to databases with machine-generated data, the legal intervention will ensure that the Database Directive could not pose an obstacle to data sharing. For example, it would not, as an additional layer of indirect protection of data, interfere with data access and data sharing. Indirectly, it would have a positive impact on the data-sharing economy, such as on innovation, research, or increased competition. The impact is expected to increase with the increasing volume of data – including machine-generated data – created and shared in the data economy.	Same as above	Same as above
Reduced litigation costs The amendment would provide a clear and stable definition of machine-generated data and explicitly exclude databases containing machine-generated data from the scope of the *sui generis* protection. This clarity would reduce the potential number of cases in courts, as well as the possibility of opportunistic litigations and the corresponding costs.	Quantitative estimates cannot be established	Affected stakeholders: Database makers and users
Reduced information and transaction costs Excluding databases containing machine-generated data removes the need to establish the database rightsholder (i.e. the database maker), which is particularly challenging in cases of joint ownership and increases the linked information and transaction costs. Making use of contract networks would also have the potential to efficiently assign database owners.	Same as above	Same as above
REFIT Cost Savings in other areas		
General cost-saving potential of horizontal rules A horizontal legal act entails lower compliance costs than sector-specific legislation. For instance, SMEs would bear unnecessarily high costs to comply with different legislation in order to participate in the relevant market.	Affected stakeholders: all groups of stakeholders covered by the Data Act. The figures below detail some of the key potential cost-saving elements brought forth by the Data Act.	
B2B/B2C contexts The increase in legal certainty (due to clear data pricing rules, definition of unfair contract terms or availability of protection against data misuse) has the potential to lower transaction costs, including legal cost. The rights of users of connected products and related services to assign the generated data to third parties will greatly reduce costs of moving between aftermarket and other service providers.	Potentially up to 68.1 billion euros (due to reduced costs of moving across aftermarket and other service providers). Other types of costs savings: not quantified.	Affected stakeholders: mostly data users, consumers
B2G context A common layer of principles to be respected in B2G data requests	Up to 155 million euros p.a. (for private	Affected stakeholders:

across the EU should decrease administrative costs and legal costs for companies (linked to current practice of lengthy negotiations and differing practices across the EU). Lower administrative burden on the public sector is expected thanks to the streamlining of the process of data acquisition (in specific situations, B2G requests will replace resource intensive procurement procedures). Public sector bodies would experience efficiency gains due to fewer resources being assigned to identify, retrieve, and process the necessary information. In the statistical domain some stakeholders expect to reduce their annual costs by 2.4 million euros (or the equivalent of 30 FTEs) by being able to use B2G mechanisms.	sector data holders due to lower costs). In the statistical domain, potential cost-saving for the public authorities of up to 64.8 million euros across the EU. Overall expected costs reduction in the public sector linked to better efficiency of up to 337 million euros p.a.	companies and public sector bodies
Cloud Edge and cloud users will spare legal and other transaction costs related to the burdensome and complicated process of the switching of data providers.	Not quantified	Affected stakeholders: companies
Interoperability All participants of the EU data spaces in all sectors should be able to decrease the transaction costs of data sharing and pooling due to the introduction or prioritisation of the relevant standards.	Not quantified	Affected stakeholders: companies

9. HOW WILL ACTUAL IMPACTS BE MONITORED AND EVALUATED?

Due to the dynamic nature of the data economy, monitoring the evolution of impacts constitutes an important part of the intervention. To ensure that the selected policy measures actually deliver the intended results and to inform possible future revisions, the Commission will set up the monitoring and evaluation process described below.

On a sectoral and macroeconomic level, the ongoing Data Market Monitoring study will assess and quantify the effects of the legal initiatives undertaken in the implementation of the EU Data Strategy with specific indicators modified to allow the economic impact of the proposal for a Data Act to be tracked, such as transaction costs related to B2B data sharing agreements. The methodology of the Data Market monitoring study will be updated to reflect the main elements of the intervention e.g., by modifying the interview questions used by the study.

Given the central role of the Common European Data Spaces in the implementation of the EU Data Strategy, many of the effects of this initiative can be usefully monitored through these data spaces as well as through insights collected by the Data Spaces Support Centre foreseen to be funded under the Digital Europe Programme. While the development of data spaces itself will be difficult to dissociate from the effects of other initiatives under the Data Strategy, the regular interaction between the Commission services, the Support Centre and the European Data Innovation Board should serve as a reliable source of information to monitor progress.

Through the Support Centre, evidence will be gathered from stakeholders on the market efficiency and effectiveness of measures taken under this initiative, such as the extent to

which the legal situation concerning data access and use rights across different sectors has improved and the impact of this initiative on real-life contractual practices.

Member States will be asked to report regularly on the efficiency and impact of the different strands of action in the data market and the extent to which public authorities engage in B2G data relationships. This will help the Commission to monitor the uptake of the measures in Member States and amongst stakeholders, also in view of compliance.

The Commission will ensure the interplay between future, relevant studies supporting new initiatives and reviews of sectoral legislation touching upon data access and sharing for the monitoring of the Data Act. At the moment, the existing data sharing structures under sectoral legislation do not offer additional sources of information for the monitoring of the Data Act due to its horizontal and novel nature.

The following table shows the chosen indicators and sources of information allowing for the monitoring of the specific objectives.

Specific objectives (see Section 4.2)	**Indicators**	**Sources of information**
Empower consumers and companies using connected products and related services.	Decrease in relevant cases brought under the dispute settlement bodies or courts (taking into account the possible initial increase in cases due to awareness). Baseline (2025): stabilized number of cases after initial increase Target (2027/2028): decrease of the baseline by 5% annually	Annual collection of information from national courts on the cases relating to data sharing agreements. For B2C, information to be derived from courts dealing with consumer law matters and from consumer protection authorities.
Increase the amount of data available for commercial and innovative use in B2B context.	SME perception of problems with data access and use: Baseline (2019): 39% of SMEs encounter difficulties with data access and use Target (5 years after adoption): 10% encounter difficulties with data access and use	Baseline: Results of SME panel consultation on B2B data-sharing principles and guidance (2019)[247]. Sources to verify the indicators: SME panel consultation to be launched 5 years after adoption Information collected from DEP funded projects by the Support Centre for Data Spaces
	a) Compliance with the provisions on the unfairness test: Baseline (2022): 0 Target (yearly): 10% increase of awareness in all sectors	Interviews and surveys by the Data Sharing Support Centre (eudatasharing.eu) and ad-hoc surveys.
Introduce new mechanisms for access to commercially-held	a) Number of requests for B2G data access issued by public authorities in the MS. b) Response time of enterprises to	Feedback from the newly created national structures for B2G data use and reuse.

[247] European Commission (2019). *SME panel consultation B2B data sharing - Final Report*.

data in exceptional situations.	data access requests. Baseline (2022): perceived situation Target (2028): improved perception	
increase the fluidity of the cloud/edge market and raise trust in the integrity of cloud and edge services	a) Fluidity of the cloud market: ➢ Number of instances that cloud users switch providers ➢ Cloud pricing	Regular reporting from the European Data Flow Monitoring Initiative Study on cloud market pricing. Survey among the relevant stakeholders.
	b) Cloud adoption in Europe Baseline (2021): 36% of EU enterprises adopts a cloud service Target (yearly growth rate in cloud adoption[248]): 10%	EUROSTAT Regular Cloud Data Reporting EU Digital Economy and Society Index, "Integration of Digital Technology" chapter.
Establish a framework for efficient data interoperability	The perception among companies as to the lack of interoperability being an obstacle to data sharing. Baseline (2021): 34% Target (2027): <10% of respondents mentioning interoperability as problem	Baseline: results of the POC on the Data Act. Surveys among businesses by the Data Spaces Support Centre, based on feedback from data spaces (self-reporting by companies).

An evaluation will also be launched to measure the performance of the initiative. This evaluation will take place 4 years after the adoption of the Data Act, which allows for the legislation to take full effect. The evaluation report will summarise and present the final results of the evaluation process, build on at least one study commissioned for this exercise, looking at all the specific objectives mentioned above as well as other studies and stakeholder input.

[248] In line with the Digital Decade Compass Target of 75% enterprise cloud adoption in Europe by 2030.

GLOSSARY

Term or acronym	*Meaning or definition*
B2B/B2C/B2G	Refers to the relation of actors engaged in data access and use: business-to-business (B2B), business-to-consumer (B2C), business-to-government (B2G).
Common European Data Space	An arrangement composed of an IT environment for secure processing of data by an open and unlimited number of organisations, and a set of legislative, administrative, and contractual rules that determine the rights of access to and processing of data.
Data	Any digital representation of acts, facts or information and any compilation of such acts, facts, or information, including in the form of sound, visual or audiovisual recording.
Data-driven innovation	The use of data and analytics to improve or create new products, services, markets, and organisational methods.
Data Governance Act (DGA)	Proposal for a Regulation of the European Parliament and of the Council on European data governance [COM/2020/767 final].
Data portability	Capacity to transfer data to which an individual or entity has a specific relationship from one IT environment (or similar) to another, based on legislative rights (e.g., Article 20 of the GDPR) or contractual agreement.
Data sharing	An act of the data holder, data producer, or data intermediary providing access to a data user for the purpose of joint or individual use of the data, based on voluntary, commercial, or non-commercial agreements, or mandatory rules. It should not be understood as making data available for free and to an undefined group of users.
Data interoperability	Refers to the ability of different digital services to work together and communicate with one another[249].
Digital Markets Act (DMA)	Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act) [COM/2020/842 final].
Digital Services Act (DSA)	Proposal for a Regulation of the European Parliament and of the Council on a Single Market for digital services (Digital Services Act) and amending Directive 2000/31/EC [COM/2020/825 final].
Free Flow of Data Regulation	Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union [OJ L 303, 28.11.2018, p.

[249] OECD (2021), Data portability, interoperability and digital platform competition, OECD Competition Committee Discussion Paper, p. 12.

	59–68].
General Data Protection Regulation (GDPR)	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 [OJ L 119, 4.5.2016, p. 1–88].
Internet of Things (IoT)	A network of physical devices, vehicles, home appliances and other items embedded with connectivity software, which enables these objects to connect and exchange data.
IaaS/SaaS/PaaS	The acronyms refer to the three main types of cloud computing services: Infrastructure as a service (IaaS), Software as a service (SaaS) and Platform as a service (PaaS). IaaS provides computing resources such as processing, storage, and networks to the users of clouds, and enables users to leverage these resources through their own implementation of virtualisation capabilities. Providers of these hardware virtual machines offer access to raw computing resources and a high degree of flexibility. IaaS users are able to access computational resources and run operating systems and software on the provided computing resources. PaaS provides users a more structured platform to deploy their own applications and services. Typically, users rely on programming languages and further tools of the cloud provider to deploy these applications. In the SaaS model, cloud users directly access the applications of the cloud provider and therefore have the convenience of not having to manage the underlying infrastructure or the capabilities of the applications.
Sui generis right	Refers to the right of the database producer protected with Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases.
SWIPO	Switching Cloud Providers and Porting Data (SWIPO), is a multi-stakeholder group facilitated by the European Commission, in order to develop voluntary Codes of Conduct for the proper application of Article 6 of the Free Flow of Data Regulation regarding the porting of non-personal data.
Switchability	Ability to move from one data processing service to another.

ANNEX 1: PROCEDURAL INFORMATION

1. Lead DG, DECIDE Planning/CWP references

The legislative proposal on the Data Act was prepared under the lead of the Directorate-General Communication Networks, Content and Technology. In the DECIDE Planning of the European Commission, the process is referred to under item PLAN/2021/10588. The Commission Work Programme for 2021 includes a legislative action for a) a Data Act and b) the review of the Database Directive, under the header "6. Data package".

2. Organisation and timing

An Inter-Service Steering Group (ISSG) assisted DG Communication Networks, Content and Technology in the preparation of the Impact Assessment and legal proposal. It included Commission services from 28 Directorate-Generals, together with the Commission's Legal Service and Secretariat General.

The work on the review of the Database Directive started with its evaluation[250], as part of the Data Package adopted in 2018. The work on the Data Act follows up on the European Strategy on Data, adopted in February 2020, which announced that the Commission would explore the need for legislative action on issues that affect relations between actors in the data economy. It also indicated the possible revision of the Database Directive.

The ISSG contributed to the initiative's preparation in December 2020 (discussion on the consultation strategy and the Inception Impact Assessment) and in March 2021 (discussion on the consultation questionnaire). Three ISSG meetings (15 July, 31 August, and 20 September 2021) covered the draft Impact Assessment before submission to the Regulatory Scrutiny Board (RSB).

An Inception Impact Assessment was published on 28 May 2021 and was open to feedback from all stakeholders on the Better Regulation Portal for a period of 4 weeks. The public online consultation was launched on 3 June and closed on 3 September 2021.

The draft Impact Assessment report and all supporting documents were submitted to the RSB on 29 September, in view of a hearing on 27 October 2021.

3. Consultation of the RSB

The RSB reviewed the Impact Assessment report on 27 October 2021 and gave a negative opinion. Based on the Board's recommendations[251], the Impact Assessment has been revised as follows.

Comments of the RSB	*How and where comments have been addressed*
(B) Summary of findings	
(1) The report lacks clarity as to the	Chapter 1 has been improved to provide more

[250] SWD(2018) 146 final.
[251] *url to be added when created*

purpose and scope of the initiative, notably precisely which situations in the data-sharing context remain unregulated and problematic.	clarity about the purposes and scope of the initiative. Specifically, section 1 elaborates on the purpose while section 1.2 details which data-sharing contexts remain unregulated and problematic. Annex 5 further explains the relationship of this initiative with other relevant legal initiatives.
(2) The report lacks a single and consistent baseline. The relationship between the two baselines used is unclear and does not sufficiently reflect future developments.	The explanation on the baselines used has been improved and detailed in Chapter 5. Specifically, section 5.1.1 clarifies the reasons for using two baselines for evaluating the impacts of the measures proposed by this initiative. Section 5.1.3 describes the baseline used to assess the impact of contractual agreements on B2B data relations, while section 5.1.2 describes the baseline against which the impact of all other measures was assessed. Throughout the report (and in particular Chapter 6), the relevant baseline has been clarified.
(3) The report lacks clarity on the precise design and content of the policy options and the measures contained therein. Various concepts and notions – notably 'fairness' and 'public interest' – are not well defined.	The description of the policy options has been sharpened and made clearer in section 5.2. A new annex – Annex 10 - provides further detailed descriptions of policy options 2 and 3 and a summary table of all policy options. Concepts and notions have been clarified throughout the text, in the glossary and in the new annexes (Annex 10 and 11). The concept of the 'unfairness test' focusing on manifestly problematic contract clauses has replaced the 'fairness test'; it is explained in detail in the new Annex 11. The concept of 'fairness' related to cloud and edge services has been explained in Chapter 2, both in the problems (2.1) and in the drivers (2.2) sections. Regarding the notion of 'public interest', the impact assessment does not aim to define it. Instead, the measures proposed for enhancing data use in B2G contexts focus on exceptional situations and data needs of public sector bodies, which would justify their requests for data for businesses. These issues are treated in

	detail in section 5.2 and Annex 10.
(4) The report is not sufficiently clear on some costs and benefits and underlying assumptions used in the impact analysis.	Chapter 6 provides a clearer and more detailed overview of the costs and benefits of the proposed measures. Underlying assumptions have been better explained both in section 5.1 and Chapter 6. Annex 4 has also been enriched by a table (in its section 1) explaining the methodology underlying the calculation of key figures.
(5) The report does not bring out clearly enough the views of different categories of stakeholders. It does not highlight the issues on which their views differ most significantly.	Chapter 6 has been restructured to better reflect the different groups of stakeholders that would be affected. Issues on which their views differ most significantly have also been highlighted in this chapter. For example, for B2G, the views of businesses have been brought out more clearly, for B2B/B2C the differing views between smaller and larger players and for cloud, the dissenting view that a legislative approach could invoke reciprocal action by third countries.
(C) What to improve	
(1) The report should provide further detail on the precise situations of data access and use that the initiative will address in each context, not least for B2G relations. It should explain why it only covers data generated by products and not by software applications. It should also explain in exactly which B2B situations the existing competition rules would not suffice, thereby necessitating targeted action. In relation to 'switchability' between cloud providers, the report should be clear that this aspect is regulated already for the hyperscalers under the Data Market Act, which covers the large share of the market. The report should better explain what	Further details on which situations of data access and use the initiative will address in each context are provided in Chapter 1, section 1 and 1.2, Annex 5 and Annex 7. The initiative is the first attempt to set horizontal principles and rights on data access and use. It would disrupt the market, bringing about tangible economic benefits but also considerable compliance burden. Accordingly, while expanding its scope beyond products (e.g., to services and software) was examined under PO3, it was not retained. The relationship between competition rules and the proposed initiative is better explained in section 1.2. The relationship between the unfairness test and competition law is explained in Annexes 10 and 11.

remains problematic and why it is important to address it.	The interplay between the proposed initiative and the Data Market Act has been further elaborated in section 1.2 as well as in Annex 5, where a dedicated table (Table 1) has been inserted for this purpose.
(2) As a broader legal scope for data sharing bears significant risks, the report should identify and analyse them specifically and explicitly. It should assess the impact it may have on other domains such as trade secrets. It should clearly address the risks of instrumentalising data for unauthorised or unintended use in all contexts and identify corresponding mitigating measures.	The report identifies and analyses in detail potential risks of data access and sharing (e.g., on security, privacy, IP rights, competition etc.) in the new dedicated Annex 8. Apart from a targeted review of the Database Directive, the proposed policy option does not modify the IPR framework, including trade secrets protection. This is explained in Chapter 1, Annex 8, and the introduction of Chapter 5. The risks have been assessed in the new dedicated Annex 8.
(3) The report grounds the baseline analysis on two separate and not necessarily converging scenarios. It should explain this duality and the underlying assumptions and assess the resulting effect on the robustness of the estimates.	The description of the baselines used has been improved and their suitability for the Impact Assessment has been assessed in Chapter 5 and the methodological annex (see point 2 above). As the baseline used to assess each measure is the most relevant, this does not affect the robustness of the estimates.
(4) The report should better define the concepts and notions used. For example, the 'fairness' test, contrary to its name, does not define 'fairness' as such but rather identifies examples of 'unfairness' in grey and black-lists and a catch-all clause. The burden of proof is thus reversed – an important distinction. The report should explain how this test is going to work in practice and how the principle of contractual freedom will be respected.	The new dedicated Annex 11 provides an extensive description of the design and application of the 'unfairness test' and how and how the principle of contractual freedom is respected.
(5) The report should further detail all the measures that constitute policy options with greater precision (e.g., obligations on cloud and edge services, the definition of specific B2G reporting obligations and application of the 'once-only' principle,	The essential components of the policy options for each measure proposed have been better explained in section 5.2. In addition, a new annex (Annex 10 'Further details on the descriptions of the policy options 2 and 3') has been included that provides more detailed

compensation for data, prevention of gold-plating, etc). It should present all the essential elements of these measures in the main text (with details in the annex). It should also analyse how data sharing obligations, on contractual terms or under general access rules, would impact businesses' freedom to determine the content and terms of the contract. The general access rules should be further specified.	explanations on each of these components. Explanations regarding freedom of contract both in context of the unfairness test and the general access rules are included in Annexes 10 and 11. The general access rules, including compensation for data, are explained in detail in the new Annex 11.
(6) The report should provide clear information with regard to criteria on the concept of 'public interest' and the choice of, and rationale for, the services that have been identified for the specific policy options. It should transparently explain the seemingly arbitrary choice as to why certain areas (e.g., health or environment) are included in the preferred option while others are not (e.g., law enforcement, judicial access, housing, education, urban planning). It should clarify what is meant by 'emergencies' and whether this would include, for example, preventing or investigating a terrorist attack. It should also clarify how the once-only principle would be applied in practice and how competing information request by public authorities will be avoided. There is also a need for greater clarity on the envisaged compensation and sanction regimes. In a broader context, the report should also discuss why and in which circumstances normal acquisition of data through standard reporting obligations or procurement are not feasible. The report should also clarify who would be empowered to define and execute emergency and other data requests.	The B2G intervention area of the proposed initiative has been fundamentally reworked in the revised impact assessment, also taking into account new political guidance. B2G data use and reuse now focuses on exceptional situations where public sector bodies cannot obtain the data they need through existing mechanisms. 'Exceptional situations' includes public emergencies. Sections 2.1 and 2.3 explain the problem and the drivers respectively. Section 5.2 presents the key elements of the policy measures for B2G while further details and explanations, including an EU-level definition of 'public emergency', an explanation on the 'public interest' concept, details on the once-only principle as well as compensation for companies, are provided in Annex 10.
(7) The impact analysis should be strengthened to allow clear identification	Chapter 6 has been restructured according to stakeholder groups in order to ensure that the

of the costs and benefits for all affected groups and the macroeconomic impacts. The report should clarify which costs and benefits result directly from this initiative, which more indirectly via sectoral legislation. Consistency should be ensured in the use and applicability of various estimates of different provenance. The report should clarify the underlying assumptions and estimation methods.	impacts on each group are clear. Costs and benefits deriving from the three policy options are now assessed for businesses (section 6.2.), SMEs (section 6.3.), consumers (section 6.4) and public administrations (section 6.5). Section 6.6. focuses on the social and environmental impacts of the proposed measures. Section 6.1. specifies that the figures in Chapter 6 result only from the measures taken under the Data Act. Costs and benefits resulting from sector-specific legislation are not considered. A new table has been inserted in Annex 4 (section 1) which clarifies assumptions and provenance of the various estimates.
(8) The report should better address the simplification and burden reduction aspects. It should indicate whether and where current reporting obligations would need to be repealed or amended for the initiative not to result in additional administrative burden. Where new burdens are likely to occur, the report should identify them and clearly indicate whether overall this initiative will directly increase or reduce administrative burdens.	The REFIT table in section 8.2. has been extended to cover simplification aspects in all intervention areas of the proposed initiative. Any administrative burdens that would be incurred by the Data Act have been described in Chapters 6 and 7.
(9) The report should more transparently present the views of all relevant stakeholders and indicate how it has assessed and integrated dissenting or minority views. This would eliminate the impression that only majority views are followed.	The revised report highlights more clearly the views of all relevant stakeholders. Please see point (5) above.

The Regulatory Scrutiny Board delivered a second opinion that was positive on 21 January 2022, provided that the following recommendations were taken into account in the report.

Comments of the RSB	*How and where comments have been addressed*

(B) Summary of findings and (C) What to improve	
B(1) The report does not comprehensively explain the articulation of the initiative with other EU legislation. C(1) The report should include a comprehensive analysis of the articulation of the initiative with other EU legislation and initiatives in the same area such as the Digital Services Act.	The revised report (Chapter 1.3) includes a more comprehensive and detailed analysis of the interplay with the key legislative instruments, including the DSA.
B(2) The definition of data, its content and boundaries, as well as the extent of access to data are not clearly outlined. It is not clear why the report limits the scope for consumers and companies to connected products and related services. C(2) A clear definition of 'data', its content and boundaries should be provided. The report should clarify the issue of data ownership, relative to primary and secondary uses. C(3) The report should justify why it limits the scope for consumers and companies to data generated by connected products and related services. It should clarify why it excludes data from software or web services, which often would seem to have similar characteristics.	The introduction now incorporates the definition of data with an accompanying explanation as to its origins and justification in the context of the Data Act. The scope of the legislative instrument, including the choice to apply different requirements to the IoT scenarios and to other relationships in data economy is presented in the introductory part of Chapter 8.
B(3) The report is not sufficiently clear on the content of some of the policy options notably on the effective application of some of the concepts contained therein. C(4) Building on the clearer explanation of the dual baseline used for the analysis of impacts, the report should strengthen the description of the relationship between the two in terms of their methodological assumptions. It should also be clearer on the complementarities of the two baselines or their distinct, independent, character. C(5) Despite a better overall description of the proposed measures contained in the options, the report should provide further clarity on the various concepts and notions. These include the effective application of the once-only principle, prevention of	The content of the options has been clarified in chapter 5, the corresponding Annex 10 and Annex 11 in the case of the unfairness test. Chapter 5.1.1. has been modified to further refine the justification for and the complementarity of two distinct baselines used in the report. Notions and concepts that are not self-explanatory and were not sufficiently explained have now been presented in more detail across the text and specifically in Annex 10 which presents the content of the policy options.

gold-plating, the definition of 'reasonable compensation' and 'duly justified purpose', and the operation of the proposed 'unfairness test', as well as its articulation with DMA and DSA initiatives.	
B(4)The report lacks clarity on the conditions for data sharing in B2G situations and a more clear-cut distinction between 'exceptional situations' and 'public emergencies'. C(6) The report should be more precise on the B2G data sharing situations, clarifying whether – and how – this is predominantly a problem for businesses or for governments. The report should better frame the concept of 'exceptional situations', leaving less room for (mis)interpretation, clarifying the conditions under which these would need to be justified by the public sector bodies and better distinguishing between 'exceptional situations' and 'public emergencies', which determine whether or not the data holder receives compensation. In the same vein, the analysis should include more details on the management of public emergencies leading to request for data.	Concerning B2G situations, both the description of the problem in Chapter 2 and the content of the preferred policy option (Chapter 5, Annex 10) have been presented in a comprehensive manner. The key concepts presented therein have also been spelled out.

4. Evidence, sources, and quality

Evidence-collection process

Extensive work was carried out during the previous Commission's mandate to identify the problems that are currently preventing Europe from realising the full economic and societal potential of data-driven innovation, in particular by ensuring greater access to and use of data. This work resulted in earlier Commission policy documents[252], the consultation of stakeholders and extensive exploratory study work[253].

[252] COM/2017/9 final; COM/2018/232.

[253] Everis (2018). *Study on data sharing between companies in Europe*, Study prepared for DG CNECT; European Commission (2018c). *Study on emerging issues of data ownership, interoperability, (re-)usability and access to data, and liability*, study prepared by Deloitte; European Commission (2017). *Synopsis report consultation on the 'building a European data economy' initiative*; European Commission (2019). *SME panel consultation B2B data sharing - Final Report*; European Commission (2018). *Study to support the review of Directive 2003/98/EC on the re-use of public sector information*, study prepared by Deloitte. European Commission (2020). *Study supporting the impact assessment on the Regulation on data governance,* SMART 2019/0024, prepared by Deloitte.

A study[254] to support an Impact Assessment on enhancing the use of data in Europe was carried out.

The study[255] on model contract terms and fairness control in data sharing and in cloud contracts and on data access rights was conducted from 14 December 2020 to September 2021. The study aimed to assess possible benefits and the overall economic impact from the use of model contract terms in voluntary data sharing, including data generated by machines and the use of products, as well as in contracts for cloud services and cloud infrastructure. It also assessed the potential economic impact of a fairness test for data-sharing contracts that could possibly be included in the Data Act as well as for contracts for cloud services and cloud infrastructure that could be a part of the 'cloud rulebook' and the access conditions for the cloud services marketplace. The study also looked into possible general principles related to remuneration and other contractual conditions for data sharing and potential mechanisms for the settlement of disputes arising in the context of data-sharing contracts.

The study[256] supporting the review of Directive 96/9/EC on the legal protection of databases (Database Directive) was conducted from May to September 2021. It aimed to assist the Commission in the preparation of this Impact Assessment (problem definition, identification and assessment of policy options) and to accompany the review of the Database Directive in the context of the abovementioned Data Act. The study mainly focused on options that bring more clarity on the status of machine-generated data under the *sui generis* database right in order to facilitate access and trading in such data, so that the Database Directive supports the data economy.

The study on the economic detriment from unfair and unbalanced cloud computing contracts[257] was conducted between November 2017 and November 2018. The study's main objective was to deliver the necessary evidence to support the Commission in its assessment of the need for, and extent of, any further EU efforts to increase SMEs' trust in cloud services and allow them to reap the full potential benefits of these types of services.

The study on the legal protection of trade secrets in the context of the data economy[258] started in February 2021 and will run until April 2022. The objective of the study is to assess how the protection of trade secrets applies in the context of the data economy. The study includes 40 interviews and a survey.

[254] European Commission (2021). *Study to support this impact assessment*, SMART 2019/0024, prepared by Deloitte.
[255] European Commission (2022, *forthcoming*). *Study on model contract terms and fairness control in data sharing and in cloud contracts and on data access rights*, study prepared by ICF.
[256] European Commission (2021). *Study to support an impact assessment for the review of the Database Directive*, prepared by CE-TP-CSIL-TU.
[257] European Commission (2018). *Study on the economic detriment from unfair and unbalanced cloud computing contracts*, prepared by EY.
[258] European Commission (2021). *Study on the legal protection of trade secrets in the context of the data economy.*

The methodological support to this impact assessment on using privately held data for official statistics, a DG ESTAT exercise, provides input to the ongoing research and deliberations towards a better understanding of B2G data sharing.

Stakeholders' consultation process

Several recent stakeholder consultation processes provided input: the 2017 public consultation on building a European data economy, the 2018 public consultation on the revision of the Directive on the reuse of public sector information, the 2018 SME panel consultation on the B2B data-sharing principles and guidance, and the 2020 public consultation on the European Strategy on Data.

In addition to the broader online consultation on the data strategy[259] and on the first legal instrument on European data governance[260], the Commission published an inception impact assessment and an open public consultation on the specific questions pertaining to the Data Act, including the review of the Database Directive. The consultation actions conducted between 3 June and 3 September 2021 targeted all stakeholders and covered aspects such as data platforms, B2B data sharing, B2G data sharing for the public interest, smart contracts, rights on non-personal Internet of Things data stemming from professional use, portability for business users of cloud services, the portability right under Article 20 GDPR, Intellectual Property Rights – protection of databases and safeguards for non-personal data in international context. The results were analysed and supported the assessment of the different options.

[259] European Commission (2020). *Outcome of the online consultation on the European strategy for data*.
[260] COM/2020/767 final.

ANNEX 2: STAKEHOLDER CONSULTATION

1. Introduction

Objective of the consultation process

The open consultation collected feedback and insights from all stakeholder groups (companies, including SMEs and business associations, public authorities, academia, citizens) on measures that would create a fair data economy by ensuring better control over and conditions for data sharing.

Extensive work was initiated already during the previous Commission mandate in order to identify the problems that are currently preventing the European economy from realising the full potential of data-driven innovation. The proposal builds on past consultation actions, such as the 2017 public consultation supporting the Commission Communication on 'Building a European data economy'[261], the 2017 public consultation on the evaluation of the Database Directive, the 2018 public consultation on the revision of the Directive on the reuse of public sector information, the 2018 SME panel consultation on B2B data-sharing principles and guidance, and the Commission online open consultation on the Data strategy[262] that ran from February to May 2020.

2. Consultation actions

- *Open public consultation on the Data Act*

In line with the Better Regulation guidelines, a public online consultation was open for 12 weeks (3 June - 3 September 2021). The consultation was launched to provide input to the current initiative, and the questions therefore addressed the items covered in the initiative. It targeted all types of stakeholders and gathered input on B2B data sharing, B2G data sharing for the public interest, smart contracts, rights on non-personal Internet of Things data stemming from professional use, portability for business users of cloud services, the portability right under Article 20 GDPR, Intellectual Property Rights – protection of databases and safeguards for non-personal data in the international context.

- *Inception Impact Assessment*

An Inception Impact Assessment was published on the Better Regulation portal on 28 May 2021 and was open for feedback for 4 weeks. It also targeted all types of stakeholders. The Commission received 91 contributions on the Better Regulation Portal[263], essentially from businesses.

Other consultation actions

- *Study to support this Impact Assessment on enhancing the use of data in Europe*[264] including interviews with targeted stakeholders.

[261] COM/2017/09 final.
[262] European Commission (2020). *Outcome of the online consultation on the European strategy for data*.
[263] European Commission *webpage*: *Have your Say - Data Act & amended rules on the legal protection of databases.*
[264] European Commission (2021). *Study on enhancing the use of data*, prepared by Deloitte.

This included two cross-sectoral workshops on B2G and B2B data sharing.

- *Study on model contract terms, fairness control in data sharing and in cloud contracts and on data access rights*[265]

The focus of the study is to provide information on and evaluation of the possible economic benefits of the use of model contract terms and fairness control in B2B data sharing and cloud contracts as well incentives for data sharing. The study also aims to look into possible general principles related to remuneration and other contractual conditions for data access and potential mechanisms for the settlement of disputes which arise in the context of contracts on data sharing that could be generalised and applicable across sectors.

- *Study on the economic detriment from unfair and unbalanced cloud computing contracts*[266]

It includes an online survey of a representative sample of SMEs and start-ups that use cloud computing for the purposes of conducting their business. The study's main objective is to deliver the necessary evidence to support the Commission in its assessment of the need for, and extent of, any further EU efforts to increase SMEs' trust in cloud services and allow them to reap the full potential benefits of these types of services.

- *Study on the legal protection of trade secrets in the context of the data economy*[267]

The study is an evidence-gathering study, including the conduct of a survey and of 40 interviews. It will assess how the protection of trade secrets applies in the context of the data economy.

- *Study in support of the review of the Database Directive*[268]

This study, which included interviews with targeted stakeholders, accompanied the review of the Database Directive on the context of this Impact Assessment.

- *Methodological support to impact assessment of using privately held data by official statistics*[269]

This exercise provides input to the ongoing research and deliberations towards a better understanding of B2G data sharing.

- *Webinars on personal data platforms and industrial data platforms*

[265] European Commission (2022, *forthcoming*). *Study on model contract terms and fairness control in data sharing and in cloud contracts and on data access rights*, study prepared by ICF.
[266] European Commission (2018). *Study on the economic detriment from unfair and unbalanced cloud computing contracts*, prepared by EY.
[267] European Commission (2022), *Study on the legal protection of trade secrets in the context of the data economy*
[268] European Commission (2022). *Study in support of the review of the Database Directive*, prepared by CE-TP-CSIL-TU.
[269] ESTAT (2021). *Methodological support to impact assessment of using privately held data by official statistics*, prepared by Consulting Gruppe.

Webinars[270] were organised on 6, 7 and 8 May 2020. They brought together the relevant data platform projects in the Big Data Value Public-Private Partnership[271] portfolio.

- *Report on Business-to-Government data sharing*

The Report[272] of the High-Level Expert Group on B2G data sharing provides an analysis of the problems on B2G data sharing in the EU and offers a set of recommendations in order to ensure scalable, responsible and sustainable B2G data sharing for the public interest. In addition to the recommendation to the Commission to explore a legal framework in this area, it presents several ways to encourage private companies to share their data. These include both monetary and non-monetary incentives, for example tax incentives, investment of public funds to support the development of trusted technical tools and recognition schemes for data sharing.

- *Workshop on labels for / certification of providers of technical solutions for data exchange*

Around 100 participants from businesses (including SMEs), European institutions and academia attended this webinar on 12 May 2020. Its aim was to examine whether a labelling or certification scheme could boost the business uptake of data intermediaries by enhancing trust in the data ecosystem[273].

- *A series of workshops*

Ten workshops organised between July and November 2019 involved more than 300 stakeholders and covered different sectors. It was discussed how the organisation of data sharing in certain areas such as environment, agriculture, energy, or health could benefit society as a whole, help public actors to design better policies and improve public services, as well as private actors to produce services contributing to facing societal challenges.

- *SME Panel consultation*

This panel consultation[274], organised from October 2018 to January 2019, sought the views of SMEs on the Commission's B2B data-sharing principles and guidance issued in the April 2018 data package.

- *The latest Eurobarometer on the impact of digitisation*

This general survey on the daily lives of Europeans includes questions on people's control over and sharing of personal information. The report, published on 5 March 2020, provides information on the willingness of European citizens to share their personal information and under which conditions.

[270] BDV PPP Going Virtual – Data Platform Webinars, see *here*.
[271] European Commission, *Big Data Value Public-Private Partnership*, see *here*.
[272] European Commission, *Experts say privately held data available in the European Union should be used better and more*, see *here*.
[273] European Commission (2020). *Workshop on labels for or certification of providers of technical solutions for data exchange: Summary of discussions*, see *here*.
[274] European Commission (2019). *SME panel consultation B2B data sharing - Final Report*.

- *Opinion of the European Data Supervisor on the European strategy for data*

On 16 June 2020, the European Data Protection Supervisor adopted Opinion 3/2020 on the European strategy for data. The approach of the EDPS towards the strategy in general is positive. It considers that the implementation of the strategy will be an opportunity to set an example for an alternative data economy model.

- *Position of the Member States*

In October 2020, the European Council *'stressed the need to make high-quality data more readily available and to promote and enable better sharing and pooling of data, as well as interoperability.'* In March 2021, it recalled *'the importance of better exploiting the potential of data and digital technologies for the benefit of the society and economy.'* With regard to cloud services, in October 2020 the EU Member States unanimously adopted a Joint Declaration on building the next-generation cloud for businesses and the public sector in the EU, which calls for a next-generation EU cloud offering that reaches the highest standards, for example in portability and interoperability.

3. Main conclusions of the consultation process

The stakeholders' consultation process on data-sharing issues has been ongoing for a number of years, especially from 2017 onwards:

The 2017 public consultation[275] supporting the Communication on 'Building a European data economy' revealed that stakeholders largely agreed that more B2B data sharing would be beneficial. At the same time, they took the view that the existing regulatory framework on data sharing in B2B relations was fit for purpose. In general, stakeholders also agreed that the crucial question in B2B data sharing is not so much about data 'ownership', but about how access to data is organised.

Stakeholders strongly supported non-regulatory measures for B2B data sharing, such as (i) fostering the use of Application Programming Interfaces (APIs) for simpler and more automated access to and use of datasets; (ii) developing recommended standard contract terms; and (iii) the provision of EU-level guidance.

As part of the April 2018 Data package, the Commission put forward the Communication 'Towards a common European data space'[276], which includes *'principles to be respected in contractual practice in order to ensure fair and competitive markets for the IoT objects and for products and services that rely on non-personal machine-generated data created by such objects'* and principles that *'could support the supply of private sector data to public sector bodies under preferential conditions for reuse'*. Additionally, the Commission started the procurement process for a 'Support Centre for data sharing' to assist companies and public sector bodies in sharing private sector data by providing technical guidance and model terms of contract.

[275] European Commission (2017). *Synopsis report consultation on the 'building a European data economy' initiative*.
[276] COM(2018) 232.

A further consultation process with stakeholders, following the Communication's adoption, was launched by the Commission, including an online consultation seeking the views of SMEs. Almost 1 000 replies were received[277].

73% of the companies indicated having had difficulties in acquiring data from another company due to unfair or unreasonable practices regarding access to data (e.g., unreasonably high licensing fees, unforeseeable termination of contract). The analysis of the open question on the nature of difficulties/ practices also highlights high fees/ costs for accessing such data as the most pressing issue. Specifically, respondents from the agricultural sector highlighted this issue. The length of the process, unfavourable contracts, and technical problems in establishing contracts are issues mentioned by some respondents from the automotive and 'other manufacturing' sectors, while others from the logistics sector highlighted legal uncertainty on the matter.

A significant proportion of SMEs actively acquire data from other companies (33%) and are using (or plan to use) connected products (30%). A large majority (87%) of respondents confirm that IoT objects represent new challenges in terms of fairness in the industrial use context and just over half (54%) consider that they are currently not well addressed by law.

SMEs considered the Commission's principles on IoT objects and data coming from those objects to be useful and complete (83% of respondents). Respondents were moderately optimistic that the principles will influence contractual practice and that this in itself would be sufficient to maintain fair markets for IoT objects and data resulting from such objects. Respondents generally considered the approach based on principles to be taken up in contractual practice to be less effective in comparative terms with respect to the objective of preserving competition and avoiding data lock-ins (30% of companies considered this approach 'insufficient' or 'less sufficient').

As regards the future work of the Support Centre, all services were deemed useful, in particular those of providing a reference document on the law applicable to data sharing, guidance on data security and improving the traceability of usage of data, and industry best-practice examples.

As foreseen by the Better Regulation guidelines, an Inception Impact Assessment on the Data Act was published on 28 May 2021 and was open for feedback for 4 weeks, targeting all types of stakeholders. The Commission received 91 contributions on the Better Regulation Portal[278], essentially from businesses (business associations (47%) or companies / businesses (27%). Other types of stakeholders participated, although to a much smaller extent: academic/research institutions (6%), non-governmental organisations (4%), EU citizens (4%), consumer organisations (1%) and others (8%). Many of these stakeholders also contributed to the public online consultation. Except for

[277] European Commission (2019). *SME panel consultation B2B data sharing - Final Report*.
[278] European Commission *webpage*: *Have your Say - Data Act & amended rules on the legal protection of databases.*

four contributions from the USA, one from Iran and one from India, all other contributions came from the European Union.

The feedback dealt with all aspects and measures foreseen in the initiative, and especially with B2G and B2B data sharing.

The feedback received on the initiative in this consultation action was generally positive. The stakeholders called for a coherent framework for EU action in the field of data and for a careful articulation with existing data-related initiatives or pieces of legislation, especially in some sectors (e.g., automotive, or financial sector), as well as more general ones (e.g., GDPR, ePrivacy, Data Market Act, etc.). Many stakeholders also warned against any measure that could have the counter-productive effect to hamper innovation. Stakeholders active in the automotive sector often called for complementary measures in the car sector e.g., possibility to not only read vehicle data but also to send data to the vehicle dashboard to communicate to the driver and send data to the vehicle functions (e.g., to unlock remotely the vehicle door) in order to be able to compete with car manufacturers on the aftermarket.

A large majority of contributors commented on B2G data-sharing ideas presented in the IIA. While feedback from public sector actors support a strong framework and higher intensity option on B2G data sharing for the benefit of the society and the economy, businesses call for a cautious and flexible approach that would encourage voluntary data-sharing schemes rather than mandating them. Existing schemes in some sectors should be considered. There is a fear that unclear definition of 'public interest' could create uncertainties, so concepts need to be clearly defined and use-cases strongly argued. Stakeholders also underline the importance of incentives and reward schemes, not only monetary.

As regards B2B data sharing, most business representatives consider that such data sharing should be incentivised. If mandated, this should target situations or sectors where there is a clearly demonstrated market failure or imbalance of negotiating power between the different parties. While mostly large business representatives highlight the importance of protecting the investments made in data creation and the contractual freedom of companies, SME representatives highlight the economic benefits associated with better data access and fair data-sharing conditions. This is also a position shared by stakeholders in some sectors (construction, agriculture, after-markets in general). The concepts of a fairness test, general access modalities and model contract clauses are considered useful by numerous contributors.

The feedback given on cloud computing services confirms the problem of concentration on the cloud market, and the importance of cloud switching and data portability for users of such services and of trusted cloud environments, especially in sectors like insurance or agriculture, while some sectors already have put in place instruments in this respect (e.g., energy). The feedback exercise showed that there are very different positions regarding the question as to whether existing Codes of Conduct (aiming to make cloud computing service switching and the data portability between providers easier) are sufficient and the

process should remain led by industry, or whether a strengthened framework should be established.

As regards safeguards for non-personal data in international contexts, some stakeholders are not in favour of any provision mandating notification of exposure of EU citizens' data to foreign jurisdictions, while some other insist on the importance of transparency and are in favour of notifications and contractual commitments. Several contributors expressed concerns that any measure in this field would restrict international data flows, while underlying the importance of protecting EU citizens' data in international contexts.

Finally, several stakeholders commented on the review process of the Database Directive. Publishers are generally negative about the goals of the review of the Directive and consider the *sui generis* right should be left untouched. However, some publishing stakeholders advocated for the extension of the *sui generis* protection to databases that contain created data, such as machine-generated data. Some other stakeholders, especially NGOs, on the contrary, welcome the review and are in favour of revisiting the *sui generis* right more broadly.

The open consultation on the Data Act ran from 3 June to 3 September 2021 and covered aspects such as data platforms, B2B data sharing, B2G data sharing for the public interest, smart contracts, rights on non-personal Internet of Things data stemming from professional use, portability for business users of cloud services, the portability right under Article 20 GDPR, Intellectual Property Rights – protection of databases and safeguards for non-personal data in international context. The consultation process targeted all types of stakeholders: Member States' competent public authorities, academic and research institutions, business associations, industrial clusters, companies/businesses, consumer organisations, NGOs, trade unions and citizens.

Out of 449 respondents from 32 countries (25 Member States, Argentina, Brazil, Canada, Japan, Switzerland, United Kingdom, United States), businesses were highly represented, with 122 business associations and 105 companies/ business organisations. A hundred respondents were public authorities and 58 were citizens (56 from the EU and 2 non-EU).

The results of this online consultation (open and closed questions, as well as papers attached to the replies) were analysed along three main topics, for the purpose of this Impact Assessment: B2B data sharing (also including B2C data sharing, smart contracts, IoT, IP issues), B2G data sharing and cloud issues:

Looking at results concerning **B2B data sharing at large**, the survey confirms that most stakeholders (68%) and especially companies (91%) share data with other companies (i.e. providing data to other companies and/or accessing data from other companies), and at a high frequency ('many times' for 86% of the respondents and 91% especially for companies). This data sharing happens either on a voluntary basis (44%) or both on a mandatory and voluntary basis (48%) – with approximately similar figures when looking at companies only.

The variations in the types of data that companies access and share reflect the diversity of the data economy. The use of data leads to realised or expected benefits in terms of extra performance, better governance, development of new services and new business models, better supply chains, anticipating problems in the production line, reducing carbon footprint and increased cooperation between innovators. However, the same respondents list and describe an array of obstacles that make it difficult for the abovementioned benefits to materialise, confirming the design of the problem tree of the IA. The obstacles to B2B data sharing are both of a technical (formats, lack of standards (69%)) and legal nature (outright refusal of granting access not linked to competition concerns (55%) and abuse of contractual imbalance (44%)).

As regards *B2C data sharing*, almost 2/3 of respondents are of the opinion that manufacturers of connected products should not be able to decide unilaterally on what happens to the data generated by such products. On the contrary, respondents agree that such decisions should be taken by the owners/ users of the products instead. At the same time, respondents point to a number of limitations on the effectiveness of exercising the portability right (Article 20 of the GDPR). While most stakeholders agree that an enhanced portability right would be beneficial for consumers and innovation overall, many of them caution against the risk of strengthening the competitive advantage of gatekeeper-type organisations with well-developed capacities to collect and use data on a massive scale ('risk of EU companies becoming data donors to tech giants').

As regards *contractual fairness*, 60% of respondents agree that model contract terms could contribute to increased data sharing. Almost half of the respondents (46%) across various sectors (e.g., agriculture, construction, aftermarket, gaming, crafts, digital) agree that a contractual fairness test to avoid unilaterally imposed unfair conditions could contribute to increased data sharing, twice more than those who are against (21%). SMEs show strong support (50%) and even a significant number in the group of large companies (41%) are in favour of a fairness test (only 22% disagreed). 46% of the respondents across various sectors (e.g., aftermarket, digital, industry, gaming, financial, also representatives with cross-sectoral membership) support the horizontal data access rules applicable to data access rights established in specific sectors; only 19% disagree. While more than half of the responding micro companies and SMEs (52%) are in favour of this measure, more than a third of the representatives of large companies also agree (41%). Furthermore, organisations with cross-sectoral membership and academia support a fairness test and general access rules. Some of the doubts raised by the representatives of large businesses regarding a fairness test are related to its practicability, enforceability, different national interpretations and increase in litigation. Some respondents were concerned that general access modalities do not help much as they require the existence of a sectoral data access right.

As regards *Internet of Things*, the vast majority of respondents that had an opinion (yes: 80%; no: 20%) think that there is a market fairness problem with IoT data. Companies of all sizes share this view. Businesses are often concerned about the unfair market situation created by the manufacturers that have privileged access to IoT data. The business sector respondents, predominantly big players, who did not see market fairness to be at stake

considered that contracts and competition law sufficiently address the issue. In the papers submitted, stakeholders' opinions are inconclusive with regard to the actual intervention option. A vast majority of business associations and trade bodies (even those representing start-ups and SMEs) favour a very cautious approach. On the other hand, associations representing farmers, insurance companies or the providers of repair and aftermarket services, in particular those in the automotive sector, are clearly in favour of binding measures enhancing data portability and obliging manufacturers to allow access to the data they hold.

Finally, as regards *IP issues*, the majority of stakeholders that replied were not sure of the relationship of the Database Directive with machine-generated data. The majority of stakeholders (54%) agree that the *sui generis* right should be reviewed, in particular in relation to the status of such machine-generated data.

Looking at results of the online consultation concerning **B2G data sharing**, we observe that 68% of public authorities have experienced difficulties when requesting access to data in the context of B2G data sharing for the public interest, as compared to 30% of company/ business organisations/ associations in responding to the requests. Results also show that 91% of public authorities consider that action (EU or national) on B2G is needed (also confirmed in the submitted papers), as compared to 38% of company/ business organisations/ associations and 80% of academic/ research institutions. The main factors impeding B2G data sharing identified by public authorities are legal barriers to the use of business data for the public interest, including competition rules, lack of awareness (benefits, datasets), lack of appropriate infrastructures and cost of providing or processing such data (e.g., interoperability issues), and legal uncertainty due to different rules in Member States. Businesses consider the main factors impeding B2G data sharing to be: lack of safeguards ensuring that the data will be used only for the public interest purpose for which it was requested, lack of appropriate infrastructures, cost of providing or processing such data (e.g., interoperability issues) and commercial disincentives/ lack of incentives.

Public authorities consider B2G data sharing should be compulsory for official statistics (90%), for protecting the environment (90%) and for emergencies and crisis management, protection and resilience (86%). In these same areas, (less than) half of businesses consider that B2G data sharing should not be compulsory: data for official statistics (50%), for protecting the environment (39%) and data for emergencies and crisis management, protection and resilience (40%). This is also very much in line with the opinion of EU citizens. Also shown in their papers submitted, research institutions call for being recipients of B2G provisions of the Data Act.

The online survey also concerned **portability for business users of cloud services and safeguards for non-personal data in international context**. As regards the SWIPO codes of conducts, a minority of all responding stakeholders (39%) are aware of them. This figure is much higher when limiting the analysis to answers given by IT providers, of which 69% are aware. However, for the effectiveness of the SWIPO codes of conduct, it is particularly important that cloud customer organisations across sectors are familiar with the codes, so that a large base of customers can push large cloud providers to

declare adherence. Therefore, this level of cross-sectoral awareness is too low for the codes to be effective on the market.

When asked whether the SWIPO codes of conduct represent a suitable approach to addressing cloud service portability, most stakeholders seem unable to answer the question, with only 29% answering the question, and even fewer answering how this could best be done. This is likely the consequence of the relatively low level of awareness of the SWIPO codes of conduct and their limited implementation on the cloud market. Of the respondents, 47% of responding businesses other than IT providers consider that SWIPO codes of conduct represent a suitable approach. When limiting the analysis to IT providers themselves, this figure is much higher (69).

In the open question on what the appropriate legislative approach would be, stakeholders indicated that they see the need for a legal basis for cloud switching, but that this legislative approach should not be over prescriptive, build on standardisation and leave some flexibility for industry to fill in the rules of the necessary interoperability. 52% of respondents consider that there is a need to establish a right to portability for business users of cloud computing services in EU legislation. To 32% of respondents, high-level legal principles should be used to flesh out the data portability right, while more specific conditions of contractual, technical, commercial, and economic nature ended second.

In terms of the type of standards to be developed, respondents indicate that interoperable data formats, common data semantics and standard APIs are necessary. Standard authentication methods are also mentioned. Respondents agree that those standards should be industry-driven in an open-source process, with a number of respondents mentioning the Gaia-X initiative as a good example.

Finally, as regards safeguards for non-personal data in the international context, the majority of respondents (76%) perceives potential access to data by foreign authorities on the basis of foreign legislation as a risk to their organisation, with 19% indicating this as a big risk.

Only 0.7% of respondents state that this is not a risk at all to their company. When asked whether this potential access to data may lead to the disclosure of trade secrets or confidential business information, 74% consider this is a risk to their company, while only 4% of respondents indicate that this is not a risk at all. Also in the open questions, several respondents indicate that the potential unlawful access to data by foreign providers is a serious problem for them currently, as it reduces acceptance of their products and makes them unable to properly protect the data of their end customers.

ANNEX 3: WHO IS AFFECTED AND HOW?

1. Practical implications of the initiative

The following stakeholders will be affected by the measures:

- **Original equipment manufacturers** (OEMs) for which use of their products generates data – estimated at 300 000 private companies in the EU[279]: Medium and large OEMs will incur compliance costs, legal advice, and adaptation of their products' design; they may also fear losing their advantage in aftermarkets. Medium and large companies will incur compliance costs from increased B2G requests, but these may be offset through predictability and reduced duplication.
- **Companies and consumers using such products**: companies and consumers would get a broader choice and more efficient services. They will be able to send their products for repair to a wider range of repair services instead of needing to buy a new product[280]. For example, farmers will be able more easily to perform precision farming, to get higher yields and reduced adverse-weather induced crop losses, and to benefit from reduced costs of fertilizers and pesticides and reduced water consumption. Businesses with access to emissions data for logistics could reduce CO_2 emissions by 48%[281]. Construction companies could reduce waste by 450 to 500 million tonnes. All individual consumers would be able to access all data generated by their use of the product, not only personal data processed on the basis of consent or contract and could choose what to do with it.
- **Third party businesses that aim to reuse data generated by these products**, estimated by the European Data Market Study at around 716 000 units, are expected, through interoperability measures, to save 30% of data-processing costs and avoid loss of 40% of valuable data sharing.
- **Public sector bodies** will find it easier to obtain data held by the private sector and necessary for public interest purposes including public emergencies, protection of the environment, safeguarding public health and public statistics. For instance, access to economic loss data will produce more accurate risk assessments to inform climate adaptation.
- **Cloud service providers**: Leading cloud service providers already have in place multiple legal, technical, and organisational mitigating measures. Notification duties, certification, encryption using internal systems and role-based access controls are currently available. More advanced measures, such as 'canary clauses' or regular

[279] European Commission (2020). The European data market study update, see *website*.
[280] IEA (2019). *Energy efficiency and digitalisation*, IEA, Paris; American Council for an Energy Efficient Economy (2020). *Intelligent efficiency*; Ben Youssef, A. (2020). *How can industry 4.0 contribute to combatting climate change?* Revue d'économie industrielle, No. 169; Garetti, M. and Taisch, M. (2012). *Sustainable manufacturing: trends and research challenges*, Production Planning and Control, No. 23; European Commission (2021). *Study on enhancing the use of data*, prepared by Deloitte
[281] SWD(2020) 331 final.

reporting to customers, split processing, or independent verification by external logging service providers, are less common and will incur costs.

- **Companies using cloud services:** Costs to businesses will likely reduce as a result of the data interoperability requirements. Benefits are estimated at EUR 7.1 billion p.a.
- **SMEs:** Most aftermarket services providers are SMEs, and SMEs tend to be more reliant on data from other companies compared to large companies. They would be protected from unfair contract terms and save money on legal costs. Small and micro enterprises would generally be exempt from data-sharing obligations in the context of data generated by machines and the use of products. Small and micro companies would in principle be exempt from B2G obligations.
- **Standardisation bodies** tasked with developing interoperability standards are estimated to incur approximately EUR 1 m per standard.

2. Summary of Costs and Benefits

A summary of benefits and costs of the preferred option is given in the following tables.

I. Overview of Benefits (total for all provisions) – Preferred Option		
Description	***Amount***	***Comments***
Direct benefits		
Efficiency and productivity gains	EUR 196.7 billion p.a.	Benefits for businesses expected to be realised by 2028.
Investments	EUR 30.4 billion p.a.	Benefits for businesses and consumers.
Reduced legal costs	Not quantifiable	Benefits for businesses.
Contractual fairness	EUR 7.4 billion p.a.	Businesses, especially SMEs, are expected to benefit.
Reduced costs of moving between aftermarket and other service providers	EUR 68.1 billion p.a.	Benefit for business customers and consumers.
Reduced economic losses in emergencies	Not quantifiable	Society overall would benefit from data sharing that reduces economic losses in emergencies.
Efficiency gains from more effective environmental protection	EUR 65-93 billion p.a.	Societal and environmental benefits.
Contribution in the area of public health	EUR 76-109 billion p.a.	Societal benefit.
Efficiency gains of national structures	EUR 337 million p.a.	Public sector bodies would experience efficiency gains leading to more confidence in public services.
Lower administrative burden	EUR 155 million p.a.	Large and medium businesses would experience lower compliance costs and less duplication in B2G data sharing. Qualitative benefits include improved reputation and workforce motivation.

Demand for cloud services	EUR 7.1 billion p.a.	Expected to benefit small cloud service providers.
Confidence in cloud services	Not quantifiable	To benefit cloud service providers and to reassure 76% of users who registered concerns about extraterritorial access.
Indirect benefits		
Government revenues	EUR 96.8 billion p.a.	Societal benefits.
Additional jobs	2.2 million	Societal benefits.
Reduced emissions	Potentially 48% reductions through data-driven efficiencies in logistics.	Businesses and societal/ environmental benefits.
Reduced waste	Not quantifiable	Sensor data can identify the source of failures leading for example to a reduction of 450-500 million tonnes of waste in EU construction sector.

II. Overview of costs – Preferred option							
		Citizens/Consumers		Businesses		Administrations	
		One-off	Recurrent	One-off	Recurrent	One-off	Recurrent
Obligation of manufacturers to allow access	Direct costs	n/a	n/a	EUR 410 m n/a	EUR 88 m p.a. Max EUR 300k p.a. (per SME) Max EUR 1 m p.a. (per large company)	n/a	n/a
	Indirect costs	n/a	n/a	n/a	n/a	n/a	n/a
Ensuring contractual fairness	Direct costs	n/a	n/a	n/a	EUR 69 m p.a.	n/a	n/a
	Indirect costs	n/a	n/a	n/a	n/a	n/a	n/a
B2G data sharing	Direct costs	n/a	n/a	EUR 552.5 m	EUR 78.1 m	n/a	EUR 21.6 m p.a.
	Indirect costs	n/a	n/a	n/a	n/a	n/a	n/a
Facilitate switching between trustworthy cloud and edge services	Direct costs	n/a	n/a	n/a	n/a	n/a	n/a
	Indirect costs	n/a	n/a	n/a	n/a	n/a	n/a
Interoperability	Direct costs	n/a	n/a	n/a	n/a	EUR 1 m (per standard)	n/a
	Indirect costs	n/a	n/a	n/a	n/a	n/a	n/a

ANNEX 4: ANALYTICAL METHODS

This Impact Assessment draws on a number of studies:

- Study to support an Impact Assessment on enhancing the use of data in Europe (Deloitte) ('the support study')
- Study on model contract terms and fairness control in data sharing and in cloud contracts and on data access rights, study (ICF)
- Methodological support to impact assessment of using privately held data by official statistics (Consulting Gruppe)
- Study to support an Impact Assessment for the review of the database directive (CE-TP-CSIL-TU)

Section 1 of this annex will provide information on the assumptions, the data sources, the calculation methods as well as the analytical limitations for key estimates referenced in this Impact Assessment.

The following sections (2 to 5) will briefly outline the methodology followed in each of the abovementioned studies. Each study analysed the potential impact of a range of provisional policy options.

Policy options for this impact assessment were fine-tuned in the light of the results of the studies and the stakeholder views expressed subsequent to the completion of most of the tasks of the studies. This required conducting further quantitative and qualitative assessments. For example, the support study[282] considered two representative markets for IoT products, and this impact assessment has extrapolated those markets for wider possible impacts on the IoT market overall, according to the study's respective hypothetical efficiency gains.

1. Methodology for the calculation of key figures in this Impact Assessment

Key figure	Study	Calculation used by this study for each impact	Reference in the study
[Contracts] Annual data-related profits for data suppliers	*Study on model contract terms and fairness control in data sharing and in cloud contracts*	Breakdown of the (yearly) quantitative estimate of the baseline by the size of companies (2021-2030) of the study shows the quantitative estimation of the baseline, which is how profits of all companies would evolve in the business-as-usual scenario. The amount of data-related profits	Table 2.2

[282] European Commission (2022). *Study to support an Impact Assessment on enhancing the use of data in Europe*, prepared by Deloitte.

Key figure	Study	Calculation used by this study for each impact	Reference in the study
	and on data access rights, prepared by ICF	amounts to an average of EUR 24.7 billion per year, ranging from EUR 21.3 billion to EUR 27.1 billion over the period 2021-2030 for the baseline.	
[Contracts] Benefits and costs due to model contract terms, unfairness test and general rules on data access	*Study on model contract terms and fairness control in data sharing and in cloud contracts and on data access rights*, prepared by ICF	Benefits and costs related to the intervention measures in contracts indicate gain and loss in profits of data suppliers. Benefits over the period 2021-2030 compared to the baseline: - EUR 5.4 billion (PO1); - EUR 7.4 billion (PO2); - EUR 7.9 billion (PO3). The benefits are based on the following calculation: The baseline scenario is taken as a starting point (EUR 24.674 billion) and multiplied by using the calculated impact score of the option (1.22 for PO1). As a result, a modelled annual profit of EUR 30.057 billion (EUR 24.674 x 1.22) is calculated. This implies a benefit of the option of EUR 5.38 billion per year (PO1), this being the difference between the modelled profit under the option minus the baseline scenario. In other words, this is the improvement under the model that the option creates compared to the baseline. Costs over the period 2021-2030 compared to the baseline: - Approx. EUR 16.2 to 42 million (PO1). Hence the indication of EUR 29 million p.a. in this Chapter 6 of the IA; - Approx. EUR 56 to 82 million (PO2). Hence the indication of EUR 69 million p.a. in this	Table 8.13 (p.155) or Table 2.2, Annex 4, p. 109; Table 8.11 (p.153) or Table 2 Qualitative impacts of the policy options, Annex 4, p. 108

Key figure	Study	Calculation used by this study for each impact	Reference in the study
		Chapter 6 of the IA; - Approx. EUR 66 to 92 million (PO3). Hence the indication of EUR 79 million p.a. in this Chapter 6 of the IA. The costs indicated are expected initially only and would be significantly lower and likely marginal in subsequent years. Therefore, the assessment is limited to a qualitative appraisal of how compliance and/or enforcement costs could vary across policy options.	
Baseline in terms of EU27 GDP	*Study to support an Impact Assessment on enhancing the use of data in Europe*, prepared by Deloitte	The baseline in terms of GDP is based on the European Data Monitoring (EDM) Tool GDP projections and beyond 2025 based on GDP growth rate forecasts of the OECD (1.5%-1.6% p.a.). EDM Tool: http://datalandscape.eu/european-data-market-monitoring-tool-2018	Section 3.5.1, p. 340
[B2B/B2C] Overall GDP increase	*Study to support an Impact Assessment on enhancing the use of data in Europe*, prepared by Deloitte	The baseline scenario foresees an autonomous growth to around 13.80 trillion EUR (+20%) in 2028. For 2028, the Deloitte study analysis indicates a potential annual addition of 273.1 billion EUR to GDP if the policy option 2 intervention was introduced. If policy option 3 is introduced, a potential annual addition of 221.0 billion EUR to GDP is estimated. In 2028, the value of the GDP could increase from 13.8 trillion EUR to around 14.07 trillion EUR if the policy option 2 was introduced (plus 1.98% to the GDP). In 2028, the value of the GDP could increase from 13.80 trillion EUR to 14.02 trillion EUR if policy option 3 was introduced	Section 3.5.2, p. 343

Key figure	Study	Calculation used by this study for each impact	Reference in the study
		(plus 1.60% to the GDP). For the analysis of the economic impact a bottom-up analysis is conducted. The bottom-up approach is based on the micro-analysis of estimated impacts conducted for each of the subtasks under consideration. Within the cost-benefit-analysis, certain benefits (e.g. additional revenues, profits, productivity gains) and costs (e.g. implementation, infrastructure, compliance costs) are assessed. As far as possible, the impact on GDP is estimated based on the cost-benefit-analysis results and/or case studies. The results and estimations of the micro-analyses are extrapolated and scaled in this regard.	
[B2B/B2C] Cost savings from reduction of moving costs for aftermarket services	*Study to support an Impact Assessment on enhancing the use of data in Europe*, prepared by Deloitte	Moving costs for the users of IoT solutions for having aftermarket services from third parties, estimated to be approximately 100K EUR/year (per company/data co-producer) by the interviewed stakeholders (baseline scenario). This cost is expected to be reduced thanks to the policy measures, leading to a benefit (a saving of 15% and 20% for PO2 and PO3 respectively).	Section 3.3.3.2.2.1, p. 277;
		EUR 68 130 million p.a. (PO2 savings total vs. baseline)	Table 80, p. 287
		EUR 90 840 million p.a. (PO3 savings total vs. baseline)	Table 82, p. 292
[B2B/B2C] Gains in effectiveness and productivity due to enhanced data access and use	*Study to support an Impact Assessment on enhancing*	Baseline (GVA EU27 in 2019): EUR 1.3 billion p.a. The effectiveness/productivity is expected to increase by 15% or 10% for PO2 and PO3 respectively based on interviewed stakeholders.	Section 4.2.1.4, p. 408

Key figure	Study	Calculation used by this study for each impact	Reference in the study
	the use of data in Europe, prepared by Deloitte	EUR 196.7 billion p.a. by 2028	Table 80, p. 287
		EUR 131.2 billion p.a. across the data economy	Table 82, p. 292
[B2B/B2C] One-off and recurring costs for the development of data management agreements, in compliance with the legislation and relevant administrative/overhead cost	*Study to support an Impact Assessment on enhancing the use of data in Europe*, prepared by Deloitte	The interviewed stakeholders estimated the amount of this cost to reach approximately EUR 1 million p.a. per large company. If this were to be multiplied by the 6.190 large companies in the EU offering IoT solutions, this would lead to the conclusion of potentially very high overall costs (around EUR 6 billion p.a.). The estimates are based on the need of elaborating complex data management agreements and of tracking the use of data downstream, which is not an obligation. Under PO2, the legal and technical safeguards benefitting the data holders would considerably automatize and facilitate the implementation and monitoring of the data agreements. Furthermore, in most cases, the technical adaptations necessary to allow the access to data would not need to be introduced 'from scratch' as it is likely that most of the larger companies (i.e. those covered by PO2) would already be well equipped and technologically ready to share data on a wide scale.	Table 79, p. 284
[B2B/B2C] One-off and recurring costs for developing technical solutions	*Study to support an Impact Assessment on enhancing the use of data in Europe*, prepared by Deloitte	According to the support study, for data holders, the costs are EUR 47.8 million (one-off) and EUR 10.2 million p.a. (recurrent). For data re-users, the costs are EUR 35.6 million (one-off) and EUR 10.2 million p.a. (recurrent). As such, the total cost is EUR 83.4 million (one-off) and EUR 18 million p.a. (recurrent). The fitness tracker market is about 5% of the whole IoT market. Therefore, extrapolating the costs	Table 72, p. 267

Key figure	Study	Calculation used by this study for each impact	Reference in the study
		incurred in the fitness tracker market to the whole IoT market, the cost to develop technical solutions would total EUR 1 641 million (one-off) and EUR 354 million p.a. (recurrent). This would be the scenario under PO3. Since under PO2 there is no obligation to develop such technical solution, with a reasonable assumption that only 25% of companies choose to undertake this investment, the cost would be EUR 410 million (one-off) and EUR 88 million p.a. (recurrent).	
[B2G] Cost and benefits in terms of administrative burden for private sector due to B2G	*Study to support an Impact Assessment on enhancing the use of data in Europe,* prepared by Deloitte	The reduction of administrative burden for the private sector would be from roughly EUR 248 million to EUR 94 million. The difference between the baseline scenario, where the use cases are not streamlined and are more ad-hoc with associated time-consuming negotiation processes, and a policy intervention, which aims to facilitate B2G data collaboratives, results in costs savings for the private sector of roughly EUR 155 million ceteris-paribus. This scenario was constructed taking into account private data holders (supermarkets, commercial banks, mobile operators, accommodation platforms and ride-hailing companies) (PO2).	Section 3.3.1.4.2.2, p. 246
[B2G] Costs relating to identifying, normalising, and making data available for reuse	*Study to support an Impact Assessment on enhancing the use of data in*	The costs of both activities would amount, at the EU level, to 78.06 million euros annually. This estimate is based on the total number of affected stakeholders (data holders), required FTEs per year based on stakeholder feedback and the cost of one FTE	Section 3.3.1.4.2.1, p. 239

Key figure	Study	Calculation used by this study for each impact	Reference in the study
	Europe, prepared by Deloitte	based on the weighted annual salary of roughly EUR 45k (ICT – weighted EU27).	
[B2G] Costs for data stewards for private sector organisations	*Study to support an Impact Assessment on enhancing the use of data in Europe*, prepared by Deloitte	The costs for data stewards for the private sector amount to 68.3 million euros at the EU level (PO3). This estimate is based on the total number of affected stakeholders (data holders), required FTEs per year based on stakeholder feedback and the cost of one FTE based on the weighted annual salary of roughly EUR 45k (ICT – weighted EU27).	Section 3.3.1.5.2.1, p. 254
[B2G] Public sector costs of data steward function creation	*Study to support an Impact Assessment on enhancing the use of data in Europe*, prepared by Deloitte	The costs for the public sector to create data steward functions would amount 314.76 million euros annually at the EU level (PO3). This estimate is based on the total number of affected stakeholders (data holders), required FTEs per year based on stakeholder feedback and the cost of one FTE based on the weighted annual salary of roughly EUR 45k (ICT – weighted EU27).	Section 3.3.1.5.2.1, p. 254
[B2G] Governmental efficiency gains	*Study to support an Impact Assessment on enhancing the use of data in Europe*, prepared by Deloitte	If one would assume average efficiency gains amounting to EUR 50.000 for national authorities and EUR 20.000 for local authorities the potential savings could amount to EUR 337 million across the EU. While actual cost savings will be specific to each B2G use case, it is likely that such benefits will be reaped. The cost calculation presented above in Table 9, if one assumes 459 national public administrations (e.g., ministries, statistical offices, central banks, etc.) and 1208 local administrations (e.g., cities and local authorities) across the EU are involved in a total of 30 B2G use	Section 3.3.1.4.2.2, p. 249

Key figure	Study	Calculation used by this study for each impact	Reference in the study
		cases, each could incur some saving in terms of efficiency gains.	
[B2G] Savings for statistical offices across the EU	*Study to support an Impact Assessment on enhancing the use of data in Europe*, prepared by Deloitte	According to stakeholders interviewed, there is a potential reduction of costs after acquiring data from the private sector. For instance, it was estimated by a public-sector stakeholder that acquiring data for the calculation of their CPI from diverse companies, allowed them to reduce their annual costs by EUR2.4 million (or the equivalent of 30 FTEs). If we assume that a similar benefit could be achieved by the statistical offices in all EU Member States, there could a potential cost-saving of up to EUR 64.8 million across the EU thanks to the access to privately-held data for the calculation of the CPI.	Section 3.3.1.4.2.2, p. 248
[B2G] Costs to public sector bodies for national structures	*Study to support an Impact Assessment on enhancing the use of data in Europe*, prepared by Deloitte	These costs were based on the German Data Forum (RatSWD) which is an advisory council to the federal government with similar tasks as to those the national structure would have, according to the policy options' description. For instance, RatSWD's tasks are representation of interest of data producers and data users, advisory to legislators, event organisation, connection of research data infrastructures on a European and international level. They estimated, that convening public and private actors as decision-making body and assisting in new data access and reuse partnerships would cost approximately 10 FTEs. To oversee the legal and responsible use of data by public sector would be at least 5 FTEs in the beginning. Considering that	Section 3.3.1.4.2.2, p. 240-241

Key figure	Study	Calculation used by this study for each impact	Reference in the study
		under this policy option, Member States would be required to designate a national structure, we estimate that this structure would likely cost 21.6 million annually at the EU level, which is likely to increase the more the B2G data collaboratives are. This cost starts in 2023, as we assume the national structure would be the first step taken as a result of a regulatory intervention.	
[Cloud] Additional GDP due to increased take-up of public cloud	*Switching of cloud service providers*, prepared by International Data Cooperation (IDC) and Arthur's Legal	The expected GDP growth of additional 0.03% (PO1) and 0.05% (PO2) p.a. is calculated assuming the baseline-forecast GDP effect of cloud growth modelled in IDC's 2014 report[283] were to continue to 2025 (i.e. 0.55% effect on GDP p.a. from public cloud adoption).	Section 5.3, p. 94
[Cloud] Increase in demand for cloud due to voluntary / mandatory approach for switching cloud and edge services	*Switching of cloud service providers*, prepared by International Data Cooperation (IDC) and Arthur's Legal	According to the IDC estimates, under PO1 scenario, demand for public cloud services in the EU is projected to grow by 19.7% CAGR[284] during the period 2018-2025, rising from EUR 19.5 billion in 2018 to EUR 68.8 billion in 2025. Therefore, demand for public cloud services in the EU in 2025 shall be 6.0% higher than it would be under the baseline scenario. This represents a difference of EUR 3.9 billion in public cloud demand for 2025 between the two scenarios. Under policy option 2 scenario,	Sections 5.3.3 and 5.4.3, p. 90-91

[283] See *Final Report of the study 'SMART 2013/0043 – Uptake of Cloud in Europe'*. This is a previous analysis for the European Commission by IDC providing quantitative estimates of the impact of cloud computing on the EU economy by 2020.
[284] Compound annual growth rate.

Key figure	Study	Calculation used by this study for each impact	Reference in the study
		demand for public cloud services in the EU grows by 20.5% CAGR during the period 2018-2025, rising from EUR 19.5 billion in 2018 to EUR 71.9 billion in 2025. This means that public cloud spending in the EU in 2025 is expected to be 10.9% higher than it would be under the baseline scenario in 2025. This represents a positive difference of EUR 7.1 billion in public cloud demand for 2025 between the two scenarios.	
[Cloud] Costs to be expected from enforcement of the cloud provisions	*Internal estimate*	As a result of the concentration of the cloud market around a handful large providers, it is estimated that market monitoring will be relatively simple for NRAs (and the number of complaints may be limited, decreasing over time after initial problems will have been addressed by providers at European level. It is therefore estimated that 0.5 FTE in the national NRAs would be sufficient to undertake the cloud enforcement. Taking EUR 45K as the European average FTE cost, this would lead to a joint additional cost of EUR **585.000** for Member States at European level. Additionally, it is estimated that 0.5-1 additional FTE would be needed to coordinate the cloud supervisory issues at European level, in a cloud supervision group for NRAs. This would lead to the estimate of an additional cost of **50K** for the European Commission.	

2. Study to support an Impact Assessment on enhancing the use of data in Europe

a. Overall methodology of the study

The support study assisted the implementation of the Data Strategy, including by providing input to this impact assessment. The study was carried out in three Phases (inception, data collection, and analysis of provisional policy options). It addressed four subtasks, namely, business to government, consumer empowerment, business to business and cloud. Provisional policy options were developed as the basis for the analysis phase.

With regard to the collection of data, the key methodological and analysis tool are listed in the table below.

Tool	Details
Desk research	Desk research was a continuous exercise throughout the study and informed the stakeholder mapping, the preparation of the interview guidelines, drafting of case studies, as well as the draft reporting of findings. It provided information on the state of play and context for each subtask. It was based on academic publications, databases, and data marketplaces (e.g., Gartner, Forrester Research, Economist Intelligence Unit).
Interviews	Semi-structured interviews were conducted to collect first-hand material from key stakeholders, both on the state of play of the topic concerned and the impact of the different policy options. Interviews were particularly useful to discuss the costs and benefits of the different options. Interviews were conducted with the following types of stakeholders: • Data holders • Data (re)users • Data intermediaries
Workshops	Two workshops were organised to enable an in-depth discussion with key stakeholders on certain topics: • Business-to-business data sharing • Business-to-government data sharing
Case studies	Case studies (i.e. in-depth and detailed investigations) were carried out to demonstrate the situation in certain domains, where data sharing was effective and where not, and what types of approaches could be discerned. The studies served to define the baseline scenarios for the sub-tasks and to develop hypotheses on the impact of the policy options.
Legal and market analyses	Market and legal analyses were carried out for certain tasks to better understand the legal and business environment and data-based value chains as well as to identify the key players and key positions on the market.
Public consultation analysis	A public consultation on the Data Act was carried out from 3 June 2021 to 3 September 2021. The study report and the results of the public consultation have been used to

Tool	Details
	produce the IA staff working document prepared by the Commission.

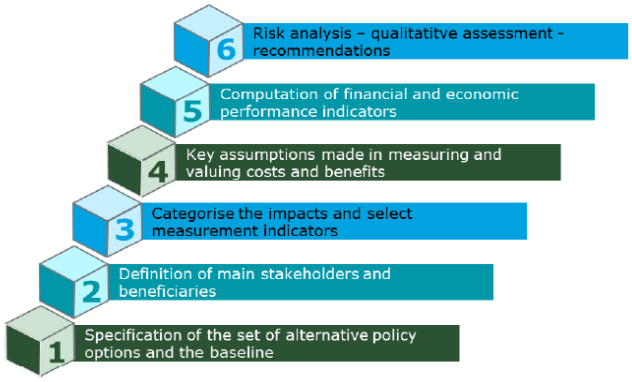
b. Data analysis activities and limitations

The data collection was hampered by the fact that the public and private sectors are still relatively new to navigating the data economy and can only share insights into for example costs and benefits to a very limited extent.

Therefore, while it was possible to collect qualitative feedback from the public and private sector on the provisional policy options for each subtask, it was more difficult to quantify their costs and benefits, e.g., because case numbers are still small, or the data sharing practices are just emerging and stakeholders themselves do not yet know their scale and/or costs of making data available. In addition, the stakeholders consulted do not yet have a final and consolidated perception on for example the potential benefits they could draw from increased data use and availabilities in their respective domain, besides speculative thoughts.

The cost-benefit analysis was elaborated individually for each of the sub-tasks. The evaluation process considered the costs and benefits for the different (main) stakeholders associated with each task. The stakeholders were divided into the following categories: data holders, data co-producers, data reusers, and data intermediaries. Impacts on society, environment, economy, and fundamental rights are also taken into account.

The key steps in the cost-benefit analysis are outlined in the figure below.



Source: Deloitte

It is in general possible to calculate the projected economic performance using the following indicators:

- Economic Net Present Value (ENPV): The ENPV is defined as the difference between the discounted total socio-economic benefits and the discounted total costs. The ENPV is comparable with the Net Present Value in financial analysis, but it also considers the broader socio-economic effects. A positive (economic) net present value indicates that the projected benefits/earnings generated by a project or investment (in present euros) exceeds the anticipated costs (also in present euros). Generally, an investment with a positive ENPV/NPV will be a

profitable one and one with a negative ENPV/NPV will result in a net loss. This concept is the basis for the Net Present Value Rule, which dictates that the only investments that should be made are those with positive NPV values.

- Economic Rate of Return (ERR): The ERR is defined as the rate that produces a zero value for the ENPV; it is comparable with the ROI (Return on investment) respectively the IRR (Internal rate of Return) in financial analysis. It is another metric commonly used as an ENPV/NPV alternative. Calculations of ERR/IRR rely on the same formula as ENPV/NPV does, except with slight adjustments. ERR/IRR calculations assume a neutral ENPV/NPV (a value of zero) and one instead solves for the discount rate. The discount rate of an investment when ENPV/NPV is zero is the investment's ERR/IRR, essentially representing the projected rate of growth for that investment. Because ERR/IRR is necessarily annual – it refers to projected returns on a yearly basis – it allows for the simplified comparison of a wide variety of types and lengths of investments.
- Benefit/Cost-ratio (B/C-ratio): The Benefit-Cost ratio is defined as the ratio between the sum of the discounted economic benefits and the sum of the discounted costs. By putting together the outcomes of the several factors analysed and calculated, it is possible to compute and interpret these three pillars of economic analysis. The different expressions are defined as follows.

Calculation of Economic Net Present Value (ENPV):

$$ENPV = \sum_{t=0}^{n} (N_t - K_t)(1+i)^{-t}$$

- N_t = *Social benefits in year t*
- K_t = *Social costs in year t*
- i = *Social discount rate (SDR)*

Calculation of Economic Rate of Return (ERR):

$$ENPV = \sum_{t=0}^{n} (N_t - K_t)(1+ERR)^{-t} = 0$$

Calculation of Economic Benefit-Cost-Ratio (EBCR):

$$EBCR = \frac{ENPV = \sum_{t=0}^{n} (N_t)(1+i)^{-t}}{ENPV = \sum_{t=0}^{n} (K_t)(1+i)^{-t}}$$

The economic performance indicators were calculated for each task as well as for each stakeholder, to the extent possible. To do so, assumptions were made, considering the limited availability of quantitative data.

Any cost-benefit analysis is based on a number of assumptions (statistical input as well as certain estimations made by the various stakeholders) that could be critical to the outcome of the analysis. As part of the risk and sensitivity analysis, the critical assumptions were identified and their effects on the outcome determined. Various sensitivity/scenario and risk analyses were performed to analyse the robustness and sensitivity of the results with regard to critical variables.

Impacts that could not be monetized were evaluated in a qualitative manner.

Quality standards for impact modelling

Specific data on costs and benefits is often scarce, inconclusive, and patchy. Any cost-benefit analysis is based on a number of assumptions (statistical input as well as certain estimations made by the various stakeholders) that could be critical to the outcome of the analysis, e.g., qualitative information to fill existing gaps. Oftentimes, these assumptions are based on expert judgment. This means that the data used in the underlying formulas is based on the best data available, challenged and refined (where necessary) by the experts of the consortium for this assignment.

Therefore, in practice, the assumptions used for the CBA are subject to an internal, in-depth peer review process. As part of this process, different assumptions are introduced in the model to compare the different outcomes. Thus, the critical assumptions are identified and their effects on the outcome are determined. This means the risk and sensitivity analysis indicates variances of economic effects as a result of changes of operational figures. Various sensitivity/scenario and risk analyses were performed to analyse the robustness and sensitivity of the results with regard to critical variables.

- The extent to which an effective sensitivity analysis can be conducted is closely linked to the quality of the CBA. Each of the abovementioned calculations was carried out within a Microsoft Excel model that was built specifically for this assignment. Deloitte's Excel models generally follow the FAST standard, consisting of practical, structured design rules for financial modelling.
- Flexible: Model design and modelling techniques must allow models to be both flexible in the immediate term and adaptable in the longer term. Models must allow users to run scenarios and sensitivities and make modifications over an extended period as new information becomes available - even by different modellers.
- Appropriate: Models must reflect key business assumptions directly and faithfully without being overbuilt or cluttered with unnecessary detail. The modeller must not lose sight of what a model is: a good representation of reality, not reality itself. Spurious precision is distracting, verging on dangerous, particularly when it is unbalanced. For example, over-specifying tax assumptions may lead to an expectation that all elements of the model are equally certain and, for example, lead to a false impression, if the revenue forecast is essentially guesswork.
- Structured: Rigorous consistency in model layout and organisation is essential to retain a model's logical integrity over time, particularly as a model's author may change. A consistent approach to structuring workbooks, worksheets and formulas saves time when building, learning, or maintaining the model.
- Transparent: Models must rely on simple, clear formulas that can be understood by other modellers and non-modellers alike. Confidence in a financial model's integrity can only be assured with clarity of logic structure and layout. Many recommendations that enhance transparency also increase the flexibility of the model to be adapted over time and make it more easily reviewed.

Multi-criteria analysis

In line with the EC's Better Regulation Guidelines, a Multi-Criteria Analysis (MCA) was carried out, in parallel to the Cost-Benefit Analysis, to identify the preferred policy option for B2B and B2C data sharing.

The MCA is a largely qualitative analysis of the policy options, based on ratings and rankings with quantitative data supporting the assessment. For this reason, MCAs accompany Cost-Benefit Analyses and Economic Modelling but do not replace them. As part of the MCA, the most significant impacts were assessed as a comparison to the baseline scenario:

- Economic impacts;
- Societal impacts; and
- Environmental impacts.

The impacts on Fundamental Rights were used as exclusion criterion.

The following criteria were taken into to assess these impacts:

- Effectiveness, i.e. the extent to which different options would achieve the objectives;
- Efficiency, i.e. comparing the benefits of the options versus the costs (incl. additional and reduced compliance costs);
- Coherence with the overarching objectives of EU policies;
- Legal and political feasibility;
- Compliance of the options with the proportionality principle.

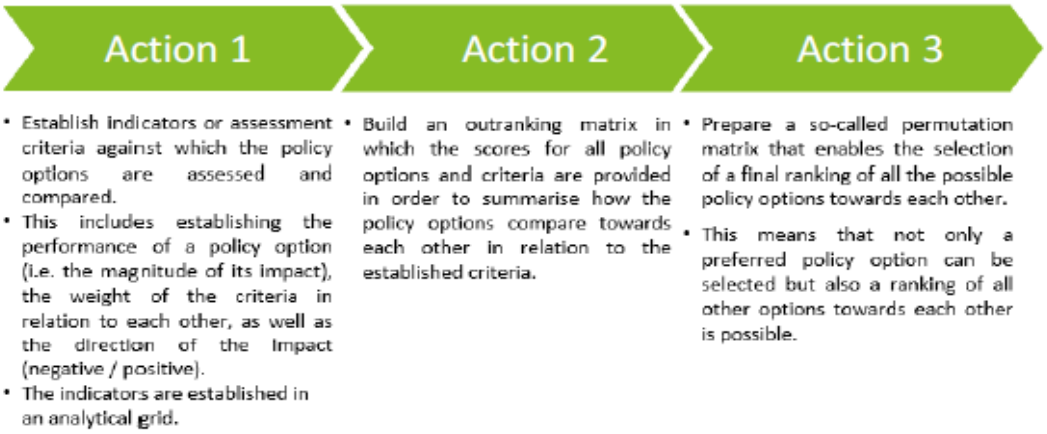
The sources of information were also defined, i.e. existing data (i.e. secondary data from other studies or databases), new data (i.e. primary data) derived from interviews, as well as the workshops.

The same assessment criteria were used for all policy options, including the baseline scenario. Using the same criteria ensures comparability across the policy options, which is imperative for the comparison of the options.

When carrying out the assessments, the expected timing of the impacts (one-off, short term, long term) was taken into account, considering changes in the baseline scenario for the specific time-frame considered.

While the impacts were assessed from the point of view of society as a whole, impacts on different groups of society (e.g. data holders, data intermediaries, data reusers) were differentiated.

The picture below summarises the key steps leading to a full MCA.



Source: Deloitte

3. Study on model contract terms and fairness control in data sharing and in cloud contracts and on data access rights (ICF)

a. Overall methodology of the study

To conduct this study, a variety of data sources was used, comprising a mix between primary data sources collected by the team, and secondary sources collected by external initiatives. The general objective was to apply a mix between micro and macro perspectives.

b. Data analysis activities

In terms of primary data collection, the main activities were the collection of data and analysis of specific data sharing cases, combined with a range of stakeholder interviews, and reinforced through a validation workshop in combination with an online survey that was open for a period of six weeks.

The initial data collection was the study of data sharing cases[285] distinguishing between one-to-one business model where a customer and service provider exchange data (unilaterally or bilaterally) – and ecosystems. The main outcome was a standardised assessment of 40 data sharing cases, examined from a contractual and business model perspective. The study captured both the legal and economic context in which the case operates (including applied contractual terms and legislative/policy context), as well as the business model that it embodies (comprising the data exploitation/valorisation strategy and the data sharing/dissemination strategy).

To achieve a representative sample the 40 cases included: service contracts governed by the legislation of 12 Member States and 4 non-Member States; service contracts from each of the key sectors referenced in the specifications (5 manufacturing, 7 mobility and traffic management, 5 agriculture, 6 smart homes);10 service contracts provided by

[285] For the purposes of this study, 'case' refers to a specific B2B data sharing contract and the corresponding business model.

SMEs, and 14 provided principally to SMEs; with a focus on use cases where the SMEs are data requestors; 16 IoT cases involving co-generated data; 5 data sharing ecosystems[286].

The baseline was further enriched by examining other sources, including notably the 2021 Report on the development of a set of recommended contract terms from the Support Centre for Data Sharing, the 2017 Legal study on Ownership and Access to Data, the 2019 Study on the Economic Detriment to Small and Medium-Sized Enterprises Arising from Unfair and Unbalanced Cloud Computing Contracts.

Additionally, 16 stakeholder interviews were organised. Finally, a validation workshop and an online survey were organised, in order to obtain further qualitative and quantitative information. Given the low participation rates, the results of the workshop and survey are interesting and informative, but ultimately not necessarily representative. Thus, primary quantitative data collection in the course of this study was largely unsuccessful.

c. Quantifying economic benefits

The main problem to be addressed by potential policy interventions is a sub-optimal level of data sharing, which would point to an untapped potential of economic benefits.

Baseline scenario

The starting point to estimate the value of data sharing is the profits of data companies. The desk research shows that data sharing is expected to grow also under the baseline scenario. The estimation of the baseline starts from data on revenues from data companies (data suppliers) from 2013 to 2020[287].

Table 1 below shows how profits of all companies would evolve in the business-as-usual scenario. The amount of data-related profits amounts to EUR 24.7 billion per year, ranging from EUR 21.3 billion to EUR 27.1 billion over the period 2021-2030, for the baseline scenario.

Table 1 Breakdown of the (yearly) quantitative estimate of the baseline by the size of companies (2021-2030), **EUR Million**

Level of impact	Baseline	Lower bound	Upper bound
SMEs	€ 17 513	€ 15 174	€ 19 337
Large	€ 7 161	€ 6 126	€ 7 807
All companies	€ 24 674	€ 21 300	€ 27 145

[286] An '**ecosystem**' is an environment where multiple stakeholders with independent and separate business activities can share and re-use data amongst each other in a many-to-many model. This implies a hub model where one or more entities act as a bridging facility to enable and enhance data sharing and use between multiple other entities.

[287] For the baseline, this study relied on the most comprehensive and available dataset on data sharing and data-related revenues offered by the IDC Data Market Study (2020).

Figure 1 Observed and extrapolated economic value of data sharing based on profits of data companies in EU27, baseline **and alternative scenarios**

Note: the blue bars show the actual profits during 2013-2020, the light green line shows a linear extrapolation of profits, the orange line represents a lower bound scenario below the baseline and the darker green line displays the upper bound scenario of the baseline. Source: ICF estimation based on IDC data.

The main limitation of this model of the baseline scenario is its starting point, namely, the revenue data of data companies. First, this data does not include the revenues from data users, which means the baseline inevitably underestimates the total value of data sharing. Our desk research provides some anecdotal evidence on the economic benefit of data sharing, and further external studies corroborate the perspective that broader social and economic benefits can be generated by enhanced data sharing. Thus, the benefit can clearly be considered a lower bound, even if data is insufficient to sustain a proper modelling exercise.

Second, the revenue data used captures the value of data-related products and services as a whole, which may be more than the economic value of data sharing per se. Hence, this may be over-estimating the true value.

Third, it is unclear from the International Data Corporation (IDC) study whether the category 'data companies' include companies who trade data as a component of their broader business activities.

Fourth, to arrive to a net value of economic benefits, this study relies on profits, rather than the turnover indicated in the IDC study, since turnover in isolation is a poor indicator of economic benefits. To do so, this study has applied a 20% profit rate to adjust revenues, reflecting a standard gross return on capital employed, before taxes, of non-financial corporations. Unfortunately, data on profits from interviews and case studies is not available. Given the general growth rates indicated in the IDC study however, there is no indication to assume that profit rates would be substantially lower that the EU market average, so that the 20% estimate is applied.

Fifth, the value of the baseline is between a lower and an upper bound, which is estimated on an assumption of lower and higher growth rates of the trends compared to the baseline from the IDC study. In the absence of evidence suggesting a particular trend, this study assumed a conservative linear trend over 2021-2030 taking a similar annual growth to the observed data points between 2013-2020, namely 5%[288]. However, to be conservative, this study has not assumed a parallel lower/higher curve respect the baseline because it is more realistic to assume the effect builds up in time.

Taking these factors into account, the ICF study adopts an anticipated annual data-related profit of € 24 674 million for data suppliers as a baseline scenario.

[288] For the lower bound it was assumed a 2.3% growth rate while a 7.5% for the upper bound. These values are based on assumptions considering that the IDC study adopt 23% on top of the baseline for the most pessimistic scenario and 75% for the most optimistic.

Quantifying the impacts of the policy options

Our desk research showed that there is no well-established metric of the economic benefit of data sharing in general. This is also corroborated by interviews in this study and confirmed by meta-analysis[289]: even participants in the data economy (i.e. those sharing data, and those receiving it) struggle to quantify the direct economic value of their data activities in terms of e.g. turnover, profit, or efficiency gains. Even if such data were available, indirect value and externalities would not be appropriately considered (such as qualitative improvements in a product or service, new functionalities, better environmental performance, etc.). These are elements that no existing study has been able to quantify reliably.

A second limitation is the difficulty to estimate a causal model that could quantitatively link specific problem drivers to specific problems – i.e. that would allow a determination of the extent to which a specific driver contributes to the problem, or from a different perspective: how much benefit could be gained by tackling a specific driver.

This is due to the lack of proper indicators for problem drivers, and the presence of many confounders. This means that the profit/revenues of data companies depend on many other factors (so-called confounders) beyond data sharing trends, such as the economic cycle, GDP, aggregate demand, business environment, competition, and innovation cycles, etc. Therefore, quantitatively identifying the precise causal effect between problem drivers, problems, and consequences (profits) is not feasible in this context.

For that reason, a second-best methodology is followed that uses qualitative assessment as an input to model the quantitative impacts on the baseline scenario. Firstly, this study identified and qualitatively assessed the main impacts that the various policy options would be expected to have. A seven-level scale was applied (ranging from --- over ~ to +++):

Table 2 Qualitative impacts of the policy options

Impact	Option 1	Option 2	Option 3
Data-driven innovation	[+] Small positive	[++] Moderate positive	[+++] Highly positive
Consumer surplus	[+] Small positive	[++] Moderate positive	[+++] Highly positive
Productivity gains	[+] Small positive	[++] Moderate positive	[++] Moderate positive
ICT skills	[+] Small positive	[++] Moderate positive	[++] Moderate positive
Tax revenues	[~] Quite uncertain or weak effect	[+] Small positive	[+] Small positive

[289] Such as the aforementioned 2013 meta-study from the OECF; see *here*.

Financial costs (compliance, admin burden)	[~] Weak effect – approx. 16.2 to 42 million EUR initially; significantly lower and likely marginal in subsequent years	[-] Small negative – approx. 56 to 82 million EUR initially; significantly lower and likely marginal in subsequent years (enforcement costs do recur)	[-] Small negative – approx. 66 to 92 million EUR initially; significantly lower and likely marginal in subsequent years in (enforcement costs do recur)
Direct and indirect economic benefits (GDP, profits, revenues)	[+] Small positive	[++] Moderate positive	[++] Moderate positive
New business model in the data economy	[~] Quite uncertain or weak effect	[+] Small positive	[+] Small positive
Competition in the data economy	[~] Quite uncertain or weak effect	[+] Small positive	[+] Small positive
Lower barriers to SMEs	[~] Quite uncertain or weak effect	[+] Small positive	[+] Small positive
Societal wellbeing	[~] Quite uncertain or weak effect	[+] Small positive	[+] Small positive

Next, this qualitative assessment was converted into a quantitative scoring, in which each impact score is determined by comparing the qualitative ranking to the baseline scenario. An equal qualitative score would result in a quantitative score of 1; a one level lower qualitative score would result in a quantitative score of 0.9, and a one level higher qualitative score would result in a quantitative score of 1.1. In other words, each quantitative score is determined purely by comparing how many levels better or worse than the baseline the policy option is form a qualitative perspective. Finally, an unweighted average impact score is calculated for each policy option, based purely on the average of all individual impact scores.

The outcome is the following table:

Table 3 Quantitative impacts of the policy options

Impact	Option 1	Option 2	Option 3
Data-driven innovation	1,3	1,4	1,5
Consumer surplus	1,3	1,4	1,5
Productivity gains	1,3	1,4	1,4
ICT skills	1,3	1,4	1,4
Tax revenues	1,2	1,3	1,3

Financial costs (compliance, admin burden)	0,9	0,8	0,8
Direct and indirect economic benefits (GDP, profits, revenues)	1,3	1,4	1,4
New business model in the data economy	1,2	1,3	1,3
Competition in the data economy	1,2	1,3	1,3
Lower barriers to SMEs	1,2	1,3	1,3
Societal wellbeing	1,2	1,3	1,3
Average impact score (unweighted, all values count equally)	1,22	1,30	1,32

Policy Option 1 scores 22% better than the baseline scenario; Policy Option 2 scores 30% better, and Policy Option 3 scores 32% better.

To translate these qualitative improvements into a quantitative impact, a model is applied that builds on the hypothesis that a qualitative improvement of a given percentage (22%, 30% and 32% in the calculations above) will translate into an equivalent impact on the baseline scenario. While by necessity an oversimplification, the approach is plausible since it takes into consideration some of the main points of uncertainty. Notably, the IDC data that was used to determine the baseline scenario already considered all of the factors that could make the revenue of data suppliers increase in the future, including those not related to the data economy (e.g. general GDP growth), thus creating a certain empirical stability. Moreover, by applying percentage increases to the baseline, the challenge of known and unknown confounders mentioned above is mitigated. Therefore, the difference between the baseline and the PO scenarios can only be attributed to the impact of the policies, as the scores are calculated only in relation to the impact factors.

Using this approach, it is possible to calculate the benefits under each policy option by increasing the baseline benefit (i.e. annual data-related profit of € 24 674 million as calculated above) by the same percentage. The calculated costs per policy option can then be deducted, in order to determine the net economic benefit of each policy option:

Table 4 Modelled benefit per policy option

	Baseline scenario	**PO1**	**PO2**	**PO3**
Baseline IDC forecast per year between 2021-2030 (in € million)	24 674	24 674	24 674	24 674
Impact score of the policy option (see table 3)	1,00 (default scenario, hence no impact)	1,22	1,30	1,32

Modelled profit (=baseline IDC forecast x impact score)	24 674	30 057	32 076	32 525
PO benefit per year in € million	N.A. (default scenario, hence no impact)	5 383	7 402	7 851
PO cost per year in € million	N.A. (default scenario, hence no impact)	29	69	79
Net PO benefit per year in € million	N.A. (default scenario, hence no impact)	5 354	7 333	7 772

Costs for the policy option have been calculated separately as averaging out at around €29 million per year, thus resulting in a net benefit of the policy option of €5 354 million (the difference between the benefit and the cost of the option). The same logic is applied to all policy options.

All policy options are expected to have a beneficial net impact compared to the baseline. Moreover, benefits increase from one policy option to the next, which is reasonably anticipated given that each policy option builds upon the previous one. As calculated in the study, around 71% of the benefits of all three policy options would accrue to SMEs, and the remaining 29% to large companies. Based on the estimated 299 000 SMEs affected, the net benefit per SME would range from around 12 700 EUR (policy option 1) to around 17 400 EUR (policy option 2) to 18 400 EUR (policy option 3).

In terms of affected industries (i.e. which sectors would benefit more than others), the impact is transversal, given the spread of data users across industries in Europe. 2020 ta indicated the following estimates of data using companies in each sector:

Industry	Data users share of total EU companies in 2020, %	2025 Baseline Scenario
Construction	2,8%	2,9%
Education	8,5%	8,8%
Financial Services	19,9%	20,9%
Healthcare	5,7%	5,9%
Information and Communications	15,6%	16,4%
Mining, Manufacturing	9,3%	9,7%
Professional services	9,4%	10,0%
Retail and Wholesale	2,6%	2,8%
Transport and Storage	13,7%	14,7%
Utilities	18,3%	19,6%
Total EU27 + U.K.	**6,8%**	**7,2%**

Since the biggest data users should reasonably benefit the most from the policies, the largest benefits would accrue with financial services (19.9%), Utilities (18.3%), ICT (15.6%), and Transport and Storage (13.7%). Benefits would likely be smallest in Retail and Wholesale (2.6%), Construction (2.8%), and Healthcare (5.7%). The overview also shows that the benefits should increase over time in all industries, since (logically) data use will continue to grow.

Thus, the benefits favour SMEs, and apply across all industries, although not at an even distribution.

The outcome represents a reasonable approximation of the anticipated impacts of each policy option, which is fairly well in line with quantitative assessments from other sources, including the IDC study. The latter identified a higher potential economic benefit under optimal policies, but this is to be expected given that the three contemplated policy options do not incorporate every conceivable measure (e.g. mandatory data sharing was not retained).

The assessment above also underwent sensitivity analysis to determine whether the outcomes would be substantially different by applying diverging weightings to the impacts, but this was found not to be the case: both the absolute amounts and the differences between policy options are relatively[290] stable.

4. Methodological support to impact assessment of using privately held data by official statistics (Consulting Gruppe)

a. Overall methodology of the study

The study was based on extensive desk research and revolves around the conceptualisation and evaluation of costs and benefits at different scales. The focus of this study was on the domain of private data sharing for official statistics (B2G4S for short) considered as a sub-domain of the private data sharing for public purposes (B2G), as illustrated in Figure 1.

The first part of the study was devoted to the **conceptualization of the relevant costs and benefits** for the following two "sectors":

- private businesses holding data that will be shared with a national statistical institute (NSI), which are denoted as PHD (for private holders of data);
- The rest of the economy (ROE) which includes everything but the PHD, i.e. it also includes society at large. It can also include businesses. For instance, if an

[290] Based on a range of test scenarios, doubling the weight of a smaller set of factors (up to 3) generally results in an impact of +/-6.5% on the policy options. By intentionally overweighting the factors that would cause the biggest changes, an impact of +/-15% can be artificially triggered. The relative differences between the policy options remain largely identical though: the standard difference between PO1 and PO3 is 0.1 impact points (the difference between the impact score of 1.22 of PO1 and 1.32 of PO3); and even with an intentional overweighting approach this difference can only be modified to 0.08, showing the stability of the model.

NSI discontinues a business survey because it has replaced it with data from certain PHDs, the businesses that were previously providing data to the survey will benefit. They will have cost savings corresponding to the avoided response burden.

The table below summarises the different types of costs and benefits that were considered in the study (and the extent of importance of each type); for detailed definitions refer to the full study report. The importance is the result of an ex-ante assessment by the authors of the study.

		PHD	**ROE**
Costs			
Recurring	Organisational	+	+
	Methodological development	+	+
	Infrastructure	+	+
	Operational	++	+++
Upfront	Organisational	+++	+++
	Methodological development	+	+++
	Infrastructure	+++	+++
	Operational	0	0
Compensation		0	+
Indirect		+	+
Benefits			
	Cost savings	+	+++
	Revenue	+	0
	Reputational	+++	0
	Improved quality of existing outputs	0	++
	Extending the line of outputs	0	++
	New outputs	0	+++
	Indirect benefits	++	+++
	Induced benefits	++	+++

Note. 0: this type of cost or benefit is not applicable for the sector in question; +: little importance; ++: medium importance; +++: high importance.

Based on such a framework, the rest of the study aims at providing rough quantitative estimates for costs and benefits for the whole B2G4S domain. In this exercise, the assessment of the benefits is considerably more challenging than the assessment of costs. Therefore, two distinct methods are adopted to quantify the benefits (graphically sketched in Figure 1):

- **Bottom-up approach**: it extrapolates from particular statistical applications to the whole B2G4S benefits, by making some assumptions about the extrapolation factors based on national experiences to date.
- **Top-down approach**: it starts with the value of all Public Sector Information and, with some assumptions of the share that official statistics represented therein, arrives at estimates of the benefits of B2G4S.

Clearly, both approaches produce figures which are subject to much uncertainty. However, both approaches lead to figures in the same order of magnitude. The valuation of costs and benefits can only be improved when actual surveys that could provide relevant data are carried out, and when more financial details emerge from national experiences as the use of private data intensifies both as substitutes for survey sources in existing statistical products or in the production of new outputs.

The study includes specific quantitative assessment for two prominent examples of statistical use-cases, namely:

- Timely statistics of mobility flows based on Mobile Network Operator (MNO) data for use in pandemic response policy.
- Consumer Price Index (CPI) based on scanner data.

The quantitative analysis of such use-cases shows that the total benefits easily exceed the total costs *in each of the considered use-cases*. Besides, they provide a basis for extrapolation in the bottom-up approach.

b. Data analysis activities

The study did not use primary data but rather sourced information from a wide range of authoritative publications including academic papers, business intelligence reports, and papers from international institutions (IDC and the Lisbon Council, McKinsey, European Commission, OECD).

5. Study to support an Impact Assessment for the review of the database directive (CE-TP-CSIL-TU)

a. Overall methodology of the study

The study was carried out in three Phases (inception, data collection, and analysis). With regard to the collection of data, the key methodological and analysis tool are listed in the table below.

Tool	Details
Desk research and literature review	Desk research took place throughout the duration of the study, with a particular focus to build up a solid knowledge base (e.g. the preparation of the interview guidelines) and identify the relevant stakeholders (stakeholder mapping). With this approach any additional information found were continuously integrated into the workflow of the study. For example, it was used to gather qualitative evidence on the expected impacts of policy options, alongside the evidence

Tool	Details
	gathered from the survey and interviews.
Legal Analysis	The study team undertook an extensive first legal analysis, both from a legal and particularly IP angle, based on desk research and literature review of recent publications related to the Database Directive and more generally the data economy and IoT environment. A second legal analysis was made in the drafting of possible policy options and their evaluation with the objective that the sui generis right of the Database Directive does not pose an obstacle to the data sharing, as foreseen by the aim of the Data Act.
Semi-targeted survey	An online survey was launched for a duration of 2 months to collect information on the applicability of the sui generis right for databases containing machine-generated databases ("MGD databases"). It also enquired on views regarding the applicability, costs and benefits of various related policy options that could improve the sharing of MGD to the benefit of society. The survey broadly targeted industries relying on Internet of Things ("IoT") as applications of IoT can be found across numerous sectors. The geographic scope covered were 12 Member States – Denmark, Finland, Sweden, Ireland, Germany, Poland, France, Austria, Romania, Bulgaria, Spain, and two third countries – UK and Turkey.
Interviews	The study team carried out individual interviews with business stakeholders, companies, or business associations, in key sectors relying on MGD to discuss and gather evidence on the support of different policy options and the costs and benefits entailed. The interviews were based on interview guidelines, which were specifically developed to ensure a coherent approach with different stakeholders.
Workshop	An online group discussion was organized in the form of a workshop with academic legal experts to receive inputs on the elaboration of the policy options.

b. Data analysis activities

Considering the legal uncertainty surrounding the Directive and use in the context of MGD, the analysis is based on empirical evidence gathered through the abovementioned collection of data: desk research, targeted survey, interviews, and a workshop. The analysis mainly relied on views of legal experts in industry, research, and academia as well as legal practitioners. Individual interviews with business stakeholders, companies, and business associations also helped to shape the results.

Quantitative estimates could not be established as there was low awareness among industry stakeholders, which may collect and use machine-generated data, of the instrument and its potential use. In addition, the sui generis database protection may be used in combination with other measures, taken by database makers to control the access and sharing of their database contents.

Due to the low application level of the *sui generis* right, complex subject matter and range of policy options, it was not possible to obtain reliable estimates on costs and

benefits expected for each policy option. As a consequence, a quantitative cost and benefit analysis was not possible to include in the study, and the assessment of policy options was based on mostly qualitative evidence.

ANNEX 5: OTHER RELEVANT LEGAL INITIATIVES

The important role of the digital platforms in the data economy is addressed by the proposal for a regulation on contestable and fair markets in the digital sector (Digital Markets Act - DMA[291]) which targets platforms acting as 'gatekeepers' in the digital sector. The proposal aims to prevent gatekeepers from imposing unfair conditions on businesses and consumers, and at ensuring the openness of important digital services.

As concerns the interplay between the DMA and the potential Data Act, two clusters of issues should be distinguished: the relation to the fairness of cloud and edge services, and the questions of access and use of data generated in the context of the use of products. As concerns the fairness of cloud and edge services, the DMA includes a provision on data portability as an obligation for businesses designated as 'gatekeepers'. While the DMA will be more far-reaching in its effect on gatekeeper platforms, the proposed legislative action under the Data Act would seek appropriate complementarity to effectively address vendor lock-in practices across the market. In particular, the Data Act would provide **a set of minimum regulatory requirements**, addressing necessary framework conditions for cloud and edge switching. These obligations could be combined with an approach of voluntary standardisation regarding the technical obstacles to switching. As such, the Data Act would be incapable of targeting specific problematic cases, e.g. where the minimum requirements do not lead to effective switching in practice because of technical complexity or commercial practices that discourage switching. This is where the DMA goes further, by imposing portability requirements to specific providers. A part of this action could be based on elements provided by the Data Act, for example making the open standards of the cloud standards repository more binding to specific services, where appropriate[292].

Table 1 – Interplay between the Data Act and DMA proposals on cloud switching

	Data Act	Digital Markets Act
Scope	Broader scope: **Cloud Switching** in general (contractual, economic, technical hurdles to cloud switching, covering portability of data and applications, as well as interoperability).	Narrower scope: **Portability of data**
Intensity of intervention	**Medium** (high-level minimum requirements for framework conditions)	**High** (more restrictive measures vis-à-vis gatekeepers)

[291] COM/2020/842 final.

[292] As an example, it could be that under the new standardisation framework of the Data Act an open API is developed specifically to migrate data from one cloud-based office suite service to another. Under the Data Act, such standards would not be mandatory. However, where problems of vendor lock-in would be discovered with an office suite of a gatekeeper platform, the DMA could mandate direct switchability by means of the aforementioned open API, turning that open standard into a binding requirement for this specific case.

Covered entities	**Horizontal market coverage:** All providers of data processing services with the primary aim to process data (typically cloud and edge services)	**Targeted coverage**: Designated gatekeeper platforms
Problems addressed	**Focus on interoperability & fluid market conditions for all entities** • Market-wide vendor lock-in practices • Loss of innovation potential due to lack of technical switching standards (open interfaces, open standards)	**Focus on market power:** • Issues with unfair market power related to vendor lock-in practices by dominant platforms.
Types of solutions presented	**Framework conditions** • Regulatory baseline presenting minimum costs, timeframes, etc. • Technical solutions through industry-led standardization.	**Concrete obligation + enforcement** • More restrictive intervention vis-à-vis gatekeeper platforms foreseen (but provisions for gatekeepers on portability under the DMA are not defined yet).

As concerns questions of access and use of data generated in the context of the use of products, the DMA provides for a series of rights of both individuals and business users vis-à-vis gatekeeper platforms. One important right is a right to effective portability of data they generate through the use of digital services offered by a gatekeeper platform on a continuous basis. For personal data, this is an enhancement of the portability right provided for under Article 20 GDPR, a right limited in a number of ways as described above[293]. The Data Act would enhance this portability right for data generated through the use of connected products, excluded from the scope of the DMA. The Data Act would, in particular, not extend other obligations foreseen for gatekeepers under the DMA, thus keeping a clear distance between the two legal regimes. Additionally, the fee regime of the Data Act would allow for parties subject to a data access obligation to charge users of the data for the investments necessary to comply with the enhancements of the portability right whereas the DMA provides for a free right of data portability. The DMA also imposes obligations on gatekeepers concerning their 'core platform services' to refrain from combining personal data sourced from these core platform services with personal data from any other services offered by the gatekeeper or with personal data from third-party services unless the data subject consents to such combination. The Data Act would be designed in such a manner consistent with the policy objective of the DMA, which is to limit the ability of gatekeepers to combine and exploit data from large numbers of users across a variety of services in order to undermine contestability and fairness in core platform services.

As far as the processing and storage of ever-increasing amounts of data are concerned, private and public entities in the EU depend increasingly on constantly evolving cloud computing deployment and service models. In this context, service providers and users have jointly developed codes of conduct to guarantee a sufficient level of portability of

[293] Section 2.1 – description of Problem 2.

data and applications between different cloud computing service providers, as mandated by the Regulation on the Free Flow of Non-Personal Data[294].

The conditions under which a private and public sector bodies can access and use personal data are provided by the **General Data Protection Regulation**[295]. The Regulation provides for a right to natural persons to port their data created by the use of a product or service, except when such data are inferred. This right applies to those personal data that are processed for the performance of a contract with the individual or when the processing is based on consent, but not when it is based on another ground for lawful processing under the Regulation. The GDPR furthermore does not provide an obligation on data controllers to have technical interfaces in place that would allow continuous sharing of data with a third party if the data subject would wish to do so as such transfer are subject to 'technical feasibility'.

The **Free Flow of Non-Personal Data Regulation**[296] ensures that non-personal data can be stored, processed and transferred anywhere in the EU. It also addresses the problem of 'vendor lock-in' at the level of providers of data processing services, by introducing self-regulatory codes of conduct to facilitate switching data between cloud services. In response, industry participants developed the 'SWIPO' codes of conduct[297].

International data processing and storage as well as data transfers are governed by the GDPR, trade commitments under the WTO (GATS) and bilateral trade agreements, in particular on computers and related services.

The **ePrivacy** rules on the processing of data in the electronic communication sector are contained in Directive 2002/58/EC currently under revision. These rules protect private life and the confidentiality of communications as well as any (personal and non-personal) data stored in and accessed from terminal equipment.

The **Platform to Business Regulation** imposes transparency obligations on platforms and requires them to inform business users about access they have (or not) to data generated through the provision of their online services. The proposal for a Digital Markets Act contains obligations in terms of the portability of data generated through gatekeeper platforms[298].

The **Open Data Directive**[299] sets out minimum rules governing the reuse of data held by the public sector and of publicly funded research data.

Sectoral legislation

In addition to the horizontal EU legal frameworks presented above, the rights and obligations on data access and use have also been regulated to various extent on the sectoral level. In the transport sector, the repair and maintenance information from motor

[294] OJ L 303, 28.11.2018, p. 59–68.
[295] OJ L 119, 4.5.2016, p. 1–88.
[296] OJ L 303, 28.11.2018, p. 59–68.
[297] OJ L 303, 28.11.2018, p. 59–68; SWIPO (2021), see *website*.
[298] OJ L 186, 11.7.2019, p. 57–79; COM/2020/842 final.
[299] OJ L 172, 26.6.2019, p. 56–83.

vehicles and agricultural machines is subject to specific data access/ sharing obligations under **type approval legislation**[300]. The EU **Electricity Regulation**[301] requires transmission system operators to provide data to regulators and for resource adequacy planning, while the EU **Electricity Directive**[302] foresees transparent and non-discriminatory procedures for access to consumption data based on interoperability requirements for data exchange developed by the Commission. The **Payment Services Directive 2**[303] opens up some types of payment transactional and account information under certain conditions, thus acting as an enabler for B2B data sharing in the area of Fintech. In the framework of the **Intelligent Transport Systems Directive (2010/40/EU)**[304], delegated regulations specify the range of data and the related procedures for the provision of road safety-related minimum universal traffic information as well as data for EU-wide real-time traffic information services. In air traffic management (ATM), non-operational data such as estimated time of arrival of flights is important to improve inter-modality and connectivity: such data would fall under the Data Act framework. However, operational real-time data related to ATM would still come under the specific regime defined in the framework of the **Single European Sky** (EC N° 549/2004, 550/2004 and 551/2004). In vessel traffic monitoring (VTM), vessel related data (tracking and tracing) such as estimated/actual time of arrival/departure of vessels is important to improve inter-modality and connectivity (port call optimisation): such data would fall under the specific regime defined in the VTMIS Directive 2002/59/EC and the High level Steering Group for Governance of the Digital Maritime System and Services (Commission Decision (EU) 2016/566 of 11 April 2016 on establishing the high-level steering group for governance of the digital maritime system and services). In the tourism sector, the relevant provisions concerning **European statistics on tourism**[305] establish a common framework for the systematic development, production, and dissemination of European statistics on tourism.

The Regulation on eco-design requirements for household washing machines and household washer-dryers (2019/2023) sets out information requirements and ensure its accessibility.

[300] OJ L 151, 14.6.2018, p. 1–218; OJ L 60, 2.3.2013, p. 1–51.
[301] OJ L 158, 14.6.2019, p. 54–124.
[302] OJ L 158, 14.6.2019, p. 125–199.
303 OJ L 337, 23.12.2015, p. 35–127.
[304] OJ L 207, 06.08.2010, p. 1-13.
[305] OJ L 192, 22.7.2011, p. 17–32.

Issues around data access and use to be tackled horizontally or by vertical instruments	
Horizontal – Data Act	Vertical – sectoral legislation
- Abuse of contractual imbalance - Empowerment of data product/service users - Obligations of data holders - Basic conditions for data access and use, including compensation for data, safeguards for data holders - Basic conditions for B2G data access - Data interoperability across sectors - Basic requirements for data processing services	- Detailed rules on cybersecurity - Technical requirements for data access (e.g. API architecture) - Issues going beyond data access and use: access to the functions of the connected device, sourcing data to the connected device - Sector-specific enforcement mechanisms - Sector-specific data formats

ANNEX 6: ON THE TARGETED REVIEW OF THE DATABASE DIRECTIVE 96/9/EC IN THE CONTEXT OF THE DATA ACT

1. Aim of the Annex

This Annex supplements the Impact Assessment. It explains the role of the protection granted to databases under the *sui generis* right enshrined in Chapter III of the Database Directive 96/9/EC and identifies the emerging challenges to the application of the *sui generis* right in the data economy. It further looks at the resulting problems leading to a possible misuse of IP rights and an accidental overprotection of databases containing machine-generated data.

Finally, it substantiates the arguments and proposes the solution for the targeted review of the *sui generis* database right in the context of the Data Act, namely to prevent the accidental and problematic expansion of *sui generis* protection to databases containing machine-generated data.

The Annex and the proposed policy intervention for the targeted review of the Database Directive are based on the evidence collected by the Commission for the preparation of the Data Act Impact Assessment, in particular the support study for the Impact Assessment[306], which assessed possible options for reviewing the Database Directive, the previous evaluation of the Database Directive in 2018 and its support study.[307] Further supporting information was also provided through the consultation activities of the support study and the Data Act, namely the Open Public Consultation[308].

2. The Background on the Database Directive

The Database Directive was adopted in February 1996. This directive provides for a two-tier structure of intellectual property protection: for original databases through copyright and a specific *sui generis* right for databases (for 'non-original' ones) if the qualitative or quantitative investment in obtaining, verifying, and presenting the data was substantial.

The aim of the *sui generis* protection is to protect the substantial investment of the database maker in setting up a database. Its objective is thereby *'to give the maker of a database the option of preventing the unauthorized extraction and/or re-utilization of all or a substantial part of the contents of that database'*[309].

Since the adoption of the Database Directive, the data economy has expanded, database technologies and automatized data production leading to machine-generated or sensor-gathered data have evolved, and investments into data in general have gained prominence. As such, the question of the application and use of the *sui generis* database right in the Data Economy is likely to become increasingly relevant.

---

[306] European Commission (2021). *Study to support an impact assessment for the review of the Database Directive*, SMART 2019/0024, prepared by CE-TP-CSIL-TU.
[307] Evaluation of Directive 96/9/EC on the legal protection of databases (Commission SWD) Brussels, 25.4.2018 SWD(2018) 146 final
[308] See feedback to the OPC on the Data Act on the European Commission webpage: Have your Say - Data Act & amended rules on the legal protection of databases.
[309] Directive 96/9/EC, Recital 41.

3. Policy developments leading to Data Act

The Commission has published two evaluations of the Database Directive since its entry into force in 1996. After the first evaluation, in 2005, the most important development was spurred by the seminal 2004 judgments of the European Court of Justice[310] that fundamentally influenced the interpretation and practice of the *sui generis* right. The ECJ ruled in cases involving football fixture lists and horse races that *sui generis* only protects investment in the collection of the data and not its creation. In many situations involving the automated creation of data, the investment has been directed towards the creation of data and not towards producing the database. Therefore, such a database should be considered a by-product of a main/ other activity. In principle, such databases should not be protected by the *sui generis* right, as they would not fulfil the 'substantial investment' criterion, as elaborated by the court.

In the Commission's 2017 Communication *on Building a European Data Economy* ('the 2017 Communication')[311], the Commission pointed out that 'raw machine-generated data' were generally not to be protected under EU intellectual property laws even though some legal uncertainty persisted among Member States. The 2017 Communication explicitly highlighted this concern vis-à-vis the *sui generis* right and announced a new evaluation process of the Database Directive. The second evaluation report of the Database Directive was published on 25 April 2018.

The 2018 Commission's evaluation report recognised some shortcomings with the *sui generis* right while concluding that a 'relatively good balance' of costs and benefits of the instrument prevailed and therefore no legislative intervention was required at that stage. However, one important area stood out for its potential to upset this balance. The evaluation report flagged that the *sui generis* right's interaction with the broader data economy was 'not fully clear at this stage and would need to be further monitored'. It also concluded that any meaningful policy intervention would need to take into account the 'policy debates around the data economy'[312].

In 2020, the Commission issued a new data Communication, entitled *A European strategy for data* ('2020 Communication') that took stock of the broader issues with the European data economy and set out the Commission's policy agenda[313]. It announced a future legislative instrument to support, among others, *'business-to-business data sharing in particular by addressing issues related to usage rights for co-generated data (such as IoT data in industrial settings), typically laid down in private contracts.'* Furthermore, it announced the review the IPR framework (including the Database Directive) in parallel to help achieve this goal of increasing the access and use of data. The 2020 Commission Communication on *Making the most of the EU's innovative potential - An intellectual property action plan to support the EU's recovery and resilience* ('The IP Action Plan')

[310] Fixtures Marketing Ltd v. Oy Veikkaus Ab (C-46/02, 9/11/2004), Fixtures Marketing Ltd v. Svenska Spel Ab (C-338/02, 9/11/2004) British Horseracing Board Ltd v. William Hill (C-203/02, 9/11/2004) Fixtures Marketing Ltd v. OPAP (C-444/02, 9/11/2004)
[311] COM(2017) 9 final.
[312] SWD(2018) 146 final, section 5.4.2.
[313] COM(2020) 66 final.

also announced a review of the *sui generis* right *'notably to facilitate the sharing of and trading in machine-generated data and data generated in the context of rolling out the IoT'*[314]. While the Data Act extends to various areas of data sharing, the most relevant for the Database Directive is the B2B context, as explained in the Impact Assessment.

The 2020 Communication led to the current Data Act proposal that aims to make more data in the EU usable to support sustainable growth and innovation by opening opportunities and removing barriers for access to data. The Data Act seeks to achieve this objective in the B2B context by focusing on the uncertainties about usage rights for data generated by machines and the use of products and on preventing imbalances among actors in the data chain, which would hinder data sharing. With the growth of the data economy, these potential problems are very likely to occur for IoT data in industrial settings, which is precisely the type of machine-generated data that the *sui generis* right has been found to have a possible accidental and problematic interaction with.

Taking into account the developments and policy work carried out by the Commission over the last years, and consistent with the stated aim of the Data Act to remove barriers for the sharing and use of data, the present targeted review of the database right specifically addresses the most relevant identified problem, namely the problematic expansion of the *sui generis* right's protection to machine-generated data.

4. The Emerging Challenge for the Database *sui generis* right

In today's context, as a consequence of the fast evolution of technologies, data is often generated in vast volumes and automatically by sensors, machines, and related technologies. With the growing rollout of IoT machinery, it becomes difficult to clearly distinguish which databases may be protected by the *sui generis* right and which may not. This is due to the fact that IoT technologies produce vast volumes of data in order to carry out their function. These data may be stored in databases, which are necessary for the operation of the machines incorporating IoT tools, for example connected cars or farming equipment. However, these databases are only a by-product of the activity carried out by the user of the connected object. Data are not, in these cases, produced to create databases but to ensure the efficient functioning of the machine. As pointed out in part 3 above, according to the seminal case law of the ECJ in 2004, databases produced incidentally in the course of an economic activity ought not to be protected by the *sui generis* right. However, without a legal intervention clarifying that machine-generated data are not covered by the *sui generis* database right, the risk exists that the current situation of unclarity as to whether machine-generated data are covered by the *sui generis* right could be opportunistically exploited by equipment manufacturers to claim IP protection beyond the intended purpose of the database protection provided for in EU law.

This risk of an expansive interpretation of the *sui generis* right to cover machine-generated data has already been documented by the 2018 Evaluation of the Database

[314] COM(2020) 760 final.

Directive, specifically with reference to the *Autobahnmaut*-case, where sensor-generated data of a road-toll system was found to be protected under the *sui generis* right[315].

The present Impact Assessment has identified a problem of imbalance in data sharing which favours data holders (i.e. the manufacturer of the machine, which contains the IoT) rather than the data users (e.g. the company operating a car fleet, which it has bought). Contrary to the Data Act's goals, the same data holders that are already in an advantageous position would benefit from the expansion of the *sui generis* right as they would be best positioned to claim this right. This would allow data holders such as original equipment manufacturers to exploit an exclusive IP right which would entitle them to prevent access to the IoT data gathered in a database to any third party, contrary to the objectives and the proposals laid down in the Data Act. In this scenario, these data holders may use their *sui generis* right in a way that leads to lock-in situations where their *de facto* monopoly over data will be backed up by a powerful *de jure* protection in the form of an IP right. The rising volume of data created automatically by machines and sensors means that, without a legislative intervention clarifying the scope of the database *sui generis* right, these risks are likely to further increase for all stakeholders involved in the data chain.

5. Policy Objective and proposed legislative intervention

In light of the above, the policy objective of the targeted review of the Database Directive is therefore to prevent the accidental and problematic expansion of IP protection, in the form of the *sui generis* right, towards machine-generated data.

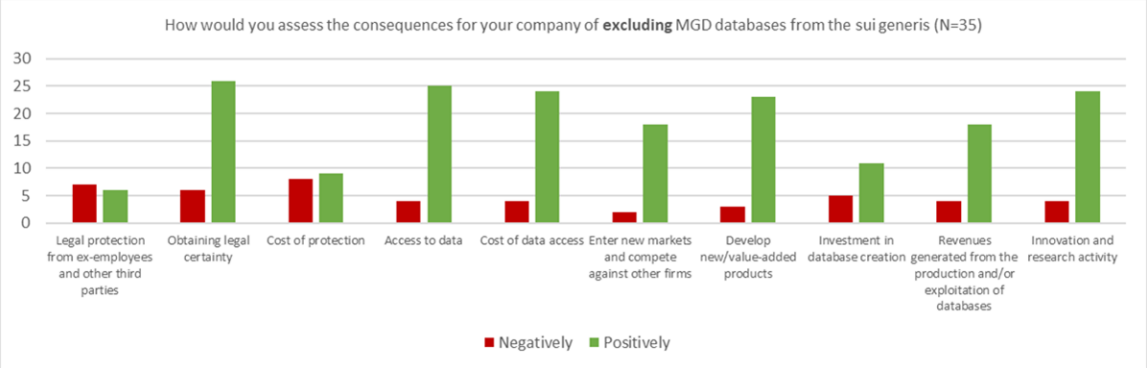
To achieve this goal, the Data Act instrument will propose (see Option 2 of the Impact Assessment) an amendment to the Database Directive (96/9/EC) to the effect that the legal protection under its Chapter III ('*Sui Generis* Right') will not extend to extraction and re-utilization of 'machine-generated data' databases which are often composed of data automatically collected or generated by machines and their embedded sensor technology.

Already in the open public consultation carried out for the 2018 evaluation of the Directive, most participants thought it was unclear whether the *sui generis* right applied to machine-generated data. A very clear majority of respondents considered a potential application of this right to machine-generated data problematic. They consider that the *sui generis* right is not appropriate for databases consisting of automatically collected or machine-generated data. The stakeholder consultation carried out in the framework of the study supporting the review of the Database Directive and the evidence collected during the consultation supports this course of action. Namely, in the survey of the study, a majority of respondents supported the option of excluding machine-generated data from *sui generis* protection. They expect this option to bring high benefits and no additional costs compared to the current situation[316] and 74% of the respondents (26 out of 35

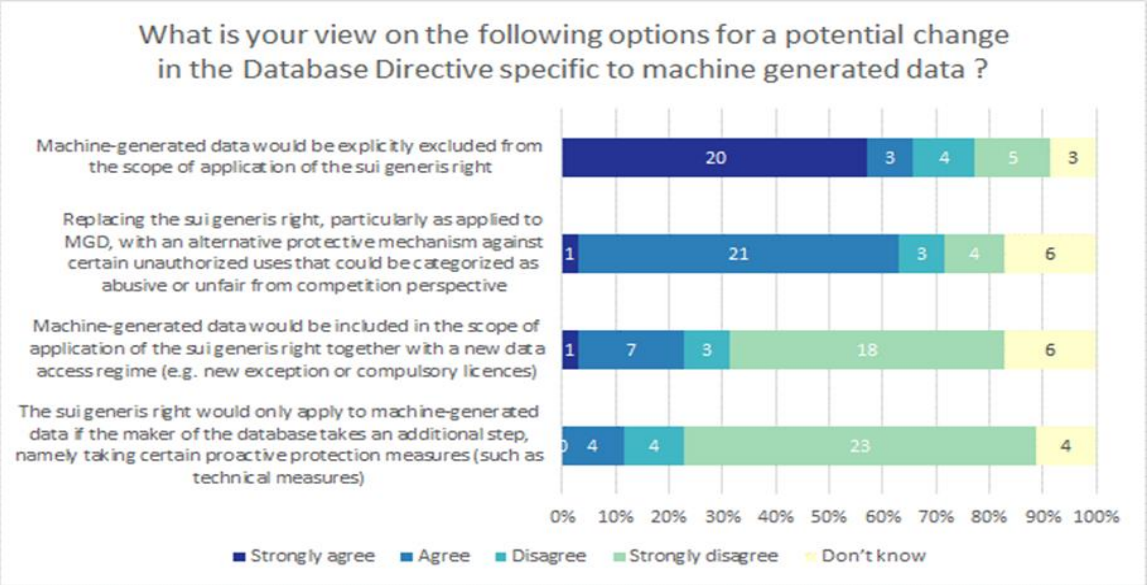
[315] *Autobahnmaut*, BGH I ZR 47/08 (25 March 2010).
[316] European Commission (2021*). Study to support an impact assessment for the review of the Database Directive*, SMART 2019/0024, prepared by CE-TP-CSIL-TU, section 4.2.

respondents) think excluding will have a positive or very positive effect on obtaining legal certainty.

***Graph 1. Respondents' opinion on excluding machine-generated data databases in the scope of the* sui generis**



Graph 2. Views on the options on a potential change in the Database Directive specific to machine-generated data



6. Expected consequences of the exclusion of machine-generated data from the *sui generis* database right

As mentioned above, the proposed intervention on the Database Directive **is coherent with the broader goals and actions of the Data Act.** Data holders, such as original equipment manufacturers, have a privileged position to use the data produced by machines, devices, and applications' operation[317]. The Data Act aims to change this by opening up businesses' and consumers' access to data they generate by using connected products and related services and, possibly, access by third parties with reasonable interest in data for innovation and competition. The status quo for the *sui generis* right, on the other hand, would potentially create problems of overly restricting access to and

[317] European Commission (2021). Study to support an impact assessment for the review of the Database Directive, SMART 2019/0024, prepared by CE-TP-CSIL-TU, section 2.1.

use of machine-generated data. Their use by third parties would likely infringe on the database right as users would often extract or reuse the whole database. This situation would be to the detriment of other database makers, users, and the general competitive interest in creating innovative products and services and become an impediment to the data economy, if applied more frequently.

Data holders of machine-generated data (IoT equipment manufacturers, IoT application providers) that may currently be in the best position to claim *sui generis* protection for machine-generated databases would not be able to claim this protection any longer. Some national legal cases, e.g. the German *Autobahnmaut*-case, have favoured the interpretation according to which machine-generated data would be included in the *sui generis* right[318], and some stakeholders in the consultation asserted that, in their view, under the status quo the protection already extends to their machine-generated databases. Nevertheless, the negative impact on these data holders should not be particularly significant in the short term as database protection of machine-generated data does not seem to be widely used as a tool to generate revenues at this stage. This intervention would be introduced at an early stage when the economy-wide IoT rollout is still only nascent. It would however prevent that in future, with the expected growth of the sensor-based data economy, the database right becomes a tool to prevent access to data in contrast with the other measures proposed in the Data Act.

Clarifying that the *sui generis* right does not apply to machine-generated data is expected to **prevent an increase in transaction costs** for the actors of the data economy which may occur if database protection is increasingly claimed on IoT data. The 2018 evaluation suggests that the legal uncertainty on the application of the *sui generis* right to machine-generated data and the possible accidental extension of IP rights over such databases would lead to an increase in transaction costs, such as legal costs to stipulate contractual agreements between makers, user-makers, and users[319]. Half of the organisations responding to the survey of the study supporting the Impact Assessment for the review of the Database Directive declared that they have encountered problems when trying to obtain access to databases containing machine-generated data. Almost two thirds of the respondents to the same survey stated that, with regard to the cost of accessing data, their companies will be negatively affected by the inclusion of the sui generis right to databases containing machine-generated data. In the open public consultation of the Data Act, the main difficulty reported in relation to interaction between the Database sui generis right and the access and use of data was the lack of clarity regarding the application of the *sui generis* right. Around half of the respondents declared themselves uncertain as regards the relation between machine-generated data and the Database Directive, and more than half of them think that it is necessary to clarify the scope of sui generis right provided by the Database Directive in relation to the status of machine-generated data. The proposal clarifying the exclusion of databases containing machine-generated data from the scope of *sui generis* protection would

[318] Autobahnmaut, BGH I ZR 47/08 (25 March 2010). See also SWD(2018) 146 final.
[319] SWD(2018) 146 final, section 5.4.2.

therefore ensure that the Directive does not become an obstacle to sharing, trading and use of data generated in the IoT environment.[320] As an immediate result, the transaction cost for data sharing, accessing and use will decrease.

The support study showed that one of the obstacles to achieve legal clarity about usage right in the data sharing context is data holders' frequent spurious claims of IP rights, such as the *sui generis* right[321]. Studies also found that data holders often use such legal protections on data or databases as an extra standard safeguard clause when sharing their data. The supporting study showed that the exclusion of machine-generated data would reduce the possibility of opportunistic litigation of third-party data use and reduce transaction costs[322].

The support study also showed that by preventing the use of the additional layer of protection to machine-generated databases, the proposal is expected to have **positive effects on competition**, as it will facilitate entry to new markets and the development of new value-added products. This solution would ease access to complete datasets for market entrants, who might use these data to develop innovative products. In the survey conducted for the support study, several respondents mentioned that access to third party data is often fundamental for the business model of companies, such as for aftermarket sales[323]. The 2018 evaluation of the Directive already highlighted such barriers to entry for potential competitors due to the *sui generis* right, in particular when competitors and interested parties need access to complete data sets to access the primary market or to compete on aftermarkets. As the support study showed, the majority of survey respondents believe that excluding machine-generated data from the *sui generis* protection will have positive effects in terms of companies entering new markets and developing new/ value-added products[324]. As remarked by more than one respondent from the automotive industry to the support study survey: *'Excluding machine-generated data from the* sui generis *right and easy access to such data would foster innovation and competition with regard to data driven business'*[325].

Finally, carving out machine-generated data from the *sui generis* database protection is **not expected to have a negative impact on the production of data and databases in the IoT context.** Both evaluations of the Directive found limited or no proof that the Database Directive has contributed to database production. The support study to this evaluation makes it clear that this is true *a fortiori* for machine-generated data: '*[t]he previous evaluation and the evidence presented in the efficiency assessment […], suggest that* sui generis *right protection of the investment in databases has no or little positive effect on incentivizing databases creation. This is even more true, for machine-generated*

[320] European Commission (2021). *Study to support an impact assessment for the review of the Database Directive*, SMART 2019/0024, prepared by CE-TP-CSIL-TU, section 4.2.
[321] European Commission (2022, *forthcoming*). *Study on model contract terms and fairness control in data sharing and in cloud contracts and on data access rights*, prepared by ICF, section 5.1.
[322] European Commission (2021). *Study to support an impact assessment for the review of the Database Directive*, SMART 2019/0024, prepared by CE-TP-CSIL-TU, section 4.2.
[323] Ibid, section 2.1.
[324] Ibid, section 4.2.
[325] Ibid.

data which in most cases are generated as a spin-off or a by-product to other main economic activities, e.g. in vehicle data.'[326] Therefore, including databases containing machine-generated data in the scope of the *sui generis* right will not result in increased production of such databases.

7. Impacts on Stakeholders

This section presents the expected impact of the legislative intervention on the Database Directive on the main stakeholders. It is mainly based on information gathered through the Data Act public consultation and from the studies and the evaluation process of the Database Directive carried out in 2018 and 2021.

The **automotive sector** includes a vast range of stakeholders on the data value chain from car manufacturers to after-market services. The impact of the intervention on these stakeholders will be potentially significant, in particular in combination with the other B2B interventions in the Data Act. Car and equipment manufacturers that are *de facto* data holders will not be able to claim *sui generis* right to protect their raw machine-generated data. On the other hand, some aftermarket and spare services will greatly benefit from the intervention as their access to data will be eased by removing one barrier of data sharing[327].

According to the Data Act public consultation, almost half of respondents (48%) from the automotive sector agreed that machine-generated data should be excluded from the *sui generis* protection, while a minority (22%) preferred expanding the protection. It is also notable that a majority of respondents (54%) from the automotive sector reported difficulties in accessing data related to the *sui generis* right.

Manufacturers at large will be impacted by the legislative intervention as far as the manufactured goods rely on data such as IoT machinery. The impact will be similar to the automotive sector. Original equipment manufacturers that are the typical *de facto* data holders will be negatively impacted by the intervention as they will not be able to claim *de jure* IP right protection in the form of *sui generis* right for their data produced through the operation of their machinery. On the other hand, businesses and consumers using these products should benefit as their access to such data will be facilitated. Moreover, third party data-seekers from other sectors will benefit the same way by an eased access right and the reduction of transaction cost in the form of avoiding opportunistic litigation from the side of the data holders.

Relatively few stakeholders answered the relevant questions for the public consultation in this stakeholder group. A clear majority had no opinion on whether to exclude machine-generated data from the *sui generis* protection or not, while the second most preferred option was the exclusion from protection.

---

[326] European Commission (2021). *Study to support an impact assessment for the review of the Database Directive*, SMART 2019/0024, prepared by CE-TP-CSIL-TU, section 4.2.

[327] Wider data access was shown to increase competition in the aftermarkets of maintenance in the car sector. See Martens, B. & Zhao, B. (2020). Data access and regime competition a case study of car data sharing in China," JRC Digital Economy Working Paper 2020-08.

The **IT sector** includes stakeholders from all parts of the data value chain. Many are data holders; others are data users but often they are both at once. The intervention will impact the sector by providing clear rules on the *sui generis* right. This is true even though the machine-generated data this intervention focuses on does typically not occur in this sector. Yet, as the intervention will help cross-sectoral third-party data access by reducing potential transaction costs of opportunistic litigation, the IT sector data-seekers will also benefit from this intervention.

Given the variety of businesses, no clear message arose from the public consultation other than that a strong majority of IT respondents were uncertain about whether the Directive applies to machine-generated data. Nevertheless, some large stakeholders voiced their support for preventing the expansion of the *sui generis* right to machine-generated data. For example a large IT company stated in its reply to the public consultation: '*To create legal clarity and business certainty for innovators, the scope of the Database Directive should expressly exclude unstructured or machine-generated data.*'

The **publishing, media and broadcasting sectors** are one of the main legacy users of the Database Directive. They rely intensely on the legal protection provided by the *sui generis* right in their business model, for example when offering commercialised database services. Therefore, they have long advocated against changing the Database Directive, including in the public consultation carried out for the Data Act where 65% of the sectors' respondents disagrees with the review of the *sui generis* right from the perspective of access and sharing of data.

However, the present legislative intervention aims at preventing the expansion of the *sui generis* right to machine-generated data and, as such, it is not expected to have a significant impact on the publishing and media industries. The intervention has a narrow focus and targets only the typically sensor-generated raw or IoT data usually in industrial settings to which the *sui generis* right ought not to apply. The type of automatically produced and processed data that the publishing and media sectors rely on will, in principle, not be affected by this review.

Finally, the **research and innovation** sector will also be impacted by the review, mainly as a data user. The impact is expected to be positive, even if its extent is difficult to measure. In the survey carried out in the context of the support study for this review, the majority of respondents saw positive effects for innovation and research activities and for revenues generated from the production and/ or exploitation of databases because of excluding machine-generated databases from the *sui generis* protection. In line with this general view, 70% of the R&D experts with a legal background that participated in the survey answered that an exclusive right covering databases containing machine-generated data would not bring considerable benefits and they also disagreed to extending the *sui generis* right to machine-generated data under certain conditions.

ANNEX 7: PROBLEMS AND SOLUTIONS

Nature of the problem	Main stakeholders and sectors	Problem in practice	Solution
• Restricted competition in the repair and maintenance aftermarkets.	Professional users as well as consumers in automotive (cars), construction (cranes), farming (milking machines), industrial engineering (robots), home appliances (smart fridge) sectors.	A factory robot breaks down. Its producer is the only entity that can access the data from the robot and that data is necessary to identify the reason for the malfunction. The company that purchased and used the robot will have to accept the repair service as offered by the robot producer, regardless of price and timeliness.	The data from the robot continues to be **streamed simultaneously to its manufacturer** but, in addition, also upon request of the user **to an industrial repair service provider**. The uninterrupted availability of data encourages **third party service providers to start offering predictive maintenance** services as well.
• Limited consumer awareness about the data collected. • Manufacturers do not share economic value of product-generated data.	Consumers using connected products in sectors including health (fitness trackers, air quality monitors), mobility (e-bikes), beauty (connected hairbrush), etc.	With each use, a connected hairbrush monitors the state of the hair and recommends corresponding cosmetic products within its brand range.	The consumer **is informed** about the data collected by the connected hairbrush and instructs the hairbrush producer to allow other specifically and explicitly chosen cosmetic brands as eligible third party to access the data from the hairbrush in real time. They suggest their own cosmetic products in competition with the producer, **increasing consumer choice**.
• Insurers unable to assess risk due to missing information about the usage of insured	Insurance companies and operators of products the use of which can lead to damage.	Car drivers pay insurance premiums based on their driving history, age, car safety features and other elements established in the	With the consent of the user, the **insurer receives data** from the car in real time and makes a number of recommendations (regarding driving

products.		contract for a longer period of time.	habits or avoiding certain areas at certain times). The **device user (driver) can modulate the level of the insurance fee** in line with this advice.
• Product users unable to innovate/improve their services due to poor access to product data.	Professional users of machines who have the capacity to analyse data.	A saw machine in a sawmill uses sensors to ensure a safe and precise cutting of timber. Sensor data are sent to the saw producer who uses it exclusively to design and sell a new sawmill machine model.	The **device user** (company operating the sawmill machine) **receives and analyses the data in real time**. The data about moisture content in wood allows it to improve the quality of the raw material. The availability of data encourages the sawmill company to **become more data savvy**.
• Product designed to limit data access by actors other than manufacturer. • Legal uncertainty about who can do what with data.	Users of devices in sectors where applicable legislation does not clarify rights to data access.	A company wishes to commercialise a new type of connected coffeemaker and sell it to a network of coffee bars. There is no sectoral legislation as to who might have the right to access and analyse the data collected by this machine. Both the producer and the owner of the bar would like to obtain exclusive rights to the data.	The Data Act clarifies that **both parties can access all data collected by the machine** and that this needs to be taken into account already at the product design level.
• Abusive use of strong negotiating power in data sharing	Sectors characterised by disparities in negotiating power between data holders and data users	An innovative start-up needs access to data from an e-bikes producer to provide a new mobility app. It abandons its plans	The start-up (**data recipient**) can invest in app development. It is **confident** that while the producer will always be in a better bargaining

	(automotive, farming, creative industries, software development).	because the producer offers a non-negotiable template contract with e.g. an unreasonable termination clause.	position, **the contractual terms will not be unfair, i.e. excessive or abusive.**
• Difficult access to private sector data in exceptional situations.	Potentially all public sector bodies, with the highest impact for those that depend on access to reliable data to fulfil their tasks (statistical offices, environment agencies).	A statistical office needs to compile consumption statistics. To achieve this, it sends questionnaires to supermarkets to collect the data. This places a considerable administrative burden on the supermarkets.	Instead of sending questionnaires, the statistical office asks supermarkets for their scanner data. Supermarkets **save time and resources** in responding to the request. The statistical office benefits from obtaining the data **quicker**.
• Difficulty in a seamless change of cloud service providers.	Potentially all sectors are concerned, with sectors where data is locked in silos particularly negatively affected: digital industries (software development), textile, retail, health.	A company wants to allow remote work for its employees. To do this, it wants to move its current data and applications to a different cloud platform. However, the contractual and commercial hurdles, as well as lack of interoperability between the platforms, means that such a cloud migration would be very costly and time consuming. The company decides to stay with its current cloud provider. Most employees are unable to work remotely.	Thanks to the Data Act there will be **no extra switching costs for users** within the cloud market. The employees can work remotely, the company becomes more efficient.

ANNEX 8: POTENTIAL RISKS OF DATA ACCESS AND SHARING

The Data Act aims to create the conditions for more data sharing between businesses, between businesses and consumers, and between businesses and public bodies. However, enhancing such data sharing and access is not without risks. These risks are analysed in this annex.

Security

Cybersecurity risks include the potential exposure of parts of an entity to incidents that disrupt the availability, integrity or confidentiality of data and information systems. Data breaches could affect an entire supply chain and essential services. Consequently, such incidents can undermine competitiveness and the ability to innovate[328]. In certain sectors, there are already specific cybersecurity requirements (e.g. as a part of the vehicle type-approval framework). Sector-specific legislation may lay down additional conditions striking the right balance between cybersecurity and access to data. The Data Act would complement actions being implemented under the EU's 2020 Cybersecurity Strategy, including the proposed reform of the Directive on Security of Network and Information Systems and the updating of the General Product Safety rules, which will include cybersecurity requirements. In particular, providers of cloud and edge services would be obliged to take technical, legal and organisational measures to prevent unlawful or unauthorised access from third countries in conflict with European legislation[329]. In addition, the measures proposed to enhance the interoperability and trustworthiness of smart contracts should minimise the chance of unlawful interference in data-sharing transactions.

Data protection breaches

Data access entails the risk of breaches in the processing of personal data[330]. Therefore, the Data Act is built in such a way that it is fully compliant with the GDPR and empowers the user by enhancing the existing data portability right provided for under Article 20 GDPR. The Data Act addresses shortcomings of this right to ensure its effectiveness to the benefit of individuals.

Intellectual property rights (IPR)

In cases where data sharing is determined through contractual agreements, the potential violation of rights can disincentive investments and innovation[331]. This is particularly true for SMEs, who might have more difficulties in identifying the right data to be shared under the right conditions, and face high risks or liabilities (e.g. fines, reputation and unsuccessful protection of intellectual property or trade secrets). However, the Data Act addresses these risks with an unfairness test for contracts to avoid the misuse of imbalances in negotiating power. It is also without prejudice to existing IPR rules and

[328] OECD, Enhancing access to and sharing of data, 2019, p. 80.
[329] IA, PO2 p. 30; PO3 p.32.
[330] OECD, Enhancing access to and sharing of data, 2019, p. 80.
[331] Idem, p. 81.

with due consideration of trade secrets protection, which means that the right holders can continue to rely on existing mechanisms to protect their rights and trade secrets.

Competition/ competitiveness

Market risks of data sharing include data spilling into the public domain or ending up in the hands of parties that can cause harm to the original data holder. As the Data Act proposal is based on the principle of user empowerment, there is a risk of misappropriation of the data by data recipients and third parties or of sharing the data with companies whose interests are in direct competition with the manufacturer of the said product. Specifically in the manufacturing sector businesses might be concerned that "sharing in European economies could be exploited by malicious actors elsewhere if not subject to proper controls" and that "exposing machines to attacks inadvertently [could] disclose commercial secrets"[332]. Indeed, some stakeholders have specifically identified the issues of data control and of legal actions against unlawful acquisition of data as highly relevant for B2B data sharing.[333] It is possible that distortions in efficient decision-making arise from asymmetric understandings of the value of datasets by different business entities. Data holders may have no incentives to share data if perceived costs are higher than expected benefits[334]. At the same time, pricing schemes in data markets can be opaque and vary according to the data user[335]. With regard to mandatory data access, the ability to compete can be undermined and the incentives to invest reduced to a level that effectively closes the possibility to enter a market[336]. This can be the case for start-ups losing their economic value when subjected to a mandatory access right. Furthermore, uncertainty about existing intellectual property rights (copyright, trade secrets, database directive) on data increases transaction costs and exposes contractual parties with a weaker negotiating power. It results in low incentives to share data or data sharing based on unfair agreements[337]. There is also a risk that opening up opportunities for data access could be exploited not solely by free riders, but mainly by the largest global tech companies to the detriment of other market actors with less access to technological infrastructure needed to acquire and get value from the data.

The Data Act would mitigate these risks in several ways:

(1) Manufacturers will retain their right to use the data and enter agreements with whomever they choose.

(2) Data holders will have the possibility to get compensation and impose conditions where they are obliged to give third parties direct access to user data.

[332] Deloitte (2018). Realising the economic potential of machine-generated, non-personal data in the EU, Report for Vodafone Group, p. 44-47.
[333] Eurochambres, Position Paper as input to the Data Act Open Public Consultation, 2 September 2021.
[334] OECD, Enhancing access to and sharing of data, 2019, p. 95.
[335] Idem. p. 96.
[336] Idem, p. 98.
[337] Idem, p. 101.

(3) Data holders will have the right to take direct action where data has been shared on the basis of incorrect or misleading information, has been accessed unlawfully or has been used for unauthorised purposes.

(4) Standardisation of secure interfaces for data sharing will be provided, as well as technical tools – such as smart contracts – that give certainty to all parties that terms of agreements will be respected and that prevent practices of data manipulation.

Rule of law

A societal risk of B2G data sharing would be an 'overreach' by the public sector, which could put the privacy of individuals at risk. The Data Act would contain the necessary safeguards to avoid this scenario and ensure a legitimate, purpose-driven, and restricted access and use of the data made available to the public sector.

Environment

Another societal risk is the environmental impact of the additional data sharing generated by the Data Act, in terms of the use of computing capacity and data storage. However, it is more likely that this risk will be exacerbated if the current trend continues, whereby most data are not being used, and are simply stored away in servers. The Commission has in fact championed initiatives to open up more data (until now, mostly public sector data[338]) as a way to help tackle environmental challenges, e.g. by better citizen awareness, promotion of data-intensive research and more efficient policy making. In addition, the increasing energy-efficiency of data infrastructures suggests that these risks are already to a large extent being addressed by technological means[339].

[338] E.g. see *here* ; and *here*.
[339] Recalibrating global data center energy-use estimates, Science 2020, see *here*.

ANNEX 9: PRELIMINARY ASSESSMENT REPORT OF THE SWIPO CODES OF CONDUCT

Executive summary[340]

- The introductory provisions in each of IaaS and the SaaS the Codes of Conduct point towards the Article 6 Objectives but in each case, the more detailed substance of the Code of Conduct seems to lose sight of these objectives. As a result**,** it is not clear that compliance with either or both Codes of Conduct results in a clear commitment from the cloud service provider to implement and maintain processes, procedures and controls that help to avoid cloud service provider lock-in and that make it easier for customers to switch between cloud service providers and port their data back to customer servers/systems.
- While each of the IaaS and SaaS Codes of Conduct are voluntary, we would expect them to be more clearly constructed as principles-based documents that reflect the Article 6 Objectives and which are supported by certain specific commitments that are directly aligned with these objectives (e.g. formats to be followed by cloud service providers for data exporting/importing, rules around determining charges and costs associated with porting and timescales for data porting). Instead, both Codes of Conduct present a wide margin of discretion for the cloud service provider to determine its own standards, procedures and processes on key issues relating to switching and porting (e.g. technical capabilities, contractual terms, associated costs, etc.) and on the limitations applied by that cloud service provider to switching and porting. The cloud service provider is then able to legitimize such standards, procedures, processes, and limitations through a transparency statement supplied pre-contract. This, however, could pave the way for potential lock-in situations.
- Also, open standards have not been taken into due account when drafting both the IaaS and SaaS Codes of Conduct. Moreover, in accordance with Article 6 Objectives of the Regulation. In this sense, the use of open standards should be stated as mandatory in the cases where required or requested by the service provider receiving the data in sections DP01 and DP05 of IaaS Code of Conduct and sections 3.2.9., 3.2.10, 3.3.9. and 3.3.10 of SaaS Code of Conduct.
- With regard to data formats and standards we suggest including a statement that participating cloud service providers agree on a technology neutral interface or certain formats that allow such exchange of data between certified cloud service providers. It is well understood that technical restrictions may apply in case of an unknown destination of the data. However, we would expect a mechanism or clear statement that all cloud service providers adhered to SWIPO Codes of Conduct do meet certain technical standards which safeguard a smooth transfer between such cloud service providers.
- Regarding data formats and standards, it is important to highlight that the IaaS Code of Conduct states that cloud service providers are not responsible for conversion or

[340] Authors: Arthur Cox LLP, DORDA Rechtsanwälte GmbH, Ramón y Cajal Abogados SLP.

translation of transferred data unless agreed with the customer or third party. This constitutes an obstacle to achieving the Article 6 Objectives.

- The same applies to the determination of charges and costs stated in section PR04 of IaaS Code of Conduct and sections 3.2.4. and 3.3.3. of SaaS Code of Conduct. It is accepted that it is not always possible to agree an upfront or fixed price to cover every possible technical implication arising from switching and/or porting but it is necessary to have certain services declared in the IaaS and SaaS Codes of Conduct as free of charge as distinct from services that do reasonably trigger a cost. In addition, both Codes of Conduct have to provide a cost scale.

- While the SaaS Code of Conduct (in section 3.2.1) requires cloud service providers to integrate a "structured process" for data export and data import respectively, it does not included wording that requires the relevant process to be designed to achieve the stated purpose of the Code of Conduct. However, the explanatory note to this section includes wording that goes beyond an aide for interpretation of the respective section and instead constitutes operative wording. It thus seems sensible to remove this operative wording from the explanatory notes and incorporate it into the relevant material sections of the SaaS Code of Conduct, as appropriate.

- The wide margin of discretion referenced above could result in varying degrees of alignment with the Article 6 Objectives across cloud service providers that adhere to one or both of the IaaS and SaaS Codes of Conduct. Put differently, the current form of each Code of Conduct presents a risk that a cloud service provider could comply with the Code of Conduct yet fail to actually put in place standards, procedures and processes that fully align with the Article 6 Objectives due to the wide margin of discretion granted to the cloud service provider under each Code of Conduct. In this respect, both Codes of Conduct, but particularly the SaaS Code of Conduct, set out some provisions as mere recommendations, whereby they should be drafted as mandatory (e.g. the CSP must provide information to the CSC regarding: (i) the policies addressing access and porting of data in the event of the provider's bankruptcy; (ii) the corresponding timescales; (iii) the network bandwidth and IT configuration, etc.

- Neither the IaaS Code of Conduct nor the SaaS Code of Conduct contain all of the minimum necessary information that can be deduced from the Article 6 Objectives of the Regulation. For instance: (i) **both Codes of Conduct** do not contain any reference to the location of data back-up; (ii) in the case of the **IaaS Code of Conduct**, the minimum network bandwidth for the porting is not included (it is just mentioned in the transparency statement as an example); (iii) in the case of the **SaaS Code of Conduct**, the procedure by which it will be updated is not defined (please, see comment 2.17) and it further leaves some information that should be drafted as mandatory to the will of the CSP as mentioned in the comment above.

- Both IaaS and SaaS Codes of Conduct include very limited requirements around the contract between the cloud service provider and the customer. The inclusion in each Code of Conduct of clearer and more substantive requirements around what must be

included in this contract (e.g. a clear commitment by the cloud service provider to comply with the relevant Code of Conduct) would enhance the alignment of each Code of Conduct with the Article 6 Objectives.

- Both the IaaS and SaaS Codes of Conduct are completely without prejudice to the GDPR. As GDPR-related challenges are not addressed this might grant CSP a loophole to reject or limit switching and/or porting requests by arguing that meeting such requests would lead to GDPR compliance issues. Such business practise could undermine the Article 6 Objectives. It might thus be worth considering if an obligation could be placed on the CSP in each Code of Conduct to take all reasonable steps required to ensure that it is not hindered from meeting the Article 6 Objectives due to applicable data protection laws provided that such obligation will not require a cloud service provider to take any action that it reasonably considers to be inconsistent with the applicable data protection laws.
- Both IaaS and SaaS Codes of Conduct do not seek to substantively address intellectual property licensing issues that may affect switching and/or porting. A failure to appropriately address such issues will undermine the ability of the Codes of Conduct to meet the Article 6 Objectives. The CSP must, at least, establish in advance which right the CSC has to acquire in order to guarantee the service and the portability of the data.
- The drafting and structure of the IaaS and SaaS Codes of Conduct differ considerably. Common structure and drafting across both Codes of Conduct would help to facilitate their practical application and understanding by customers and service providers. As to structuring the SaaS Code of Conduct could be used as role model, as to format the approach of the IaaS Code of Conduct prevails and as to level of detail a happy medium between the two Codes of Conduct would be appreciated.
- It is also important to highlight that, while the IaaS Code of Conduct is quite extensive, the SaaS Code of Conduct is shorter and there may be some unregulated issues or ambiguity. Further, the IaaS Code of Conduct's transparency statement is much more detailed than the SaaS Code of Conduct's transparency statement: for instance, it contains examples of the content that have to be included by the CSP in each section, ensuring that all necessary information is given to the CSCs. This comes as a surprise as we do expect that the data porting will be much more difficult and subject to more factual restrictions as to SaaS services which are much more unharmonized and more commonly used in the market.
- In order to protect the customer in line with the Regulations, both the IaaS and SaaS Codes of Conduct should establish a minimum period during which the customer's data will remain available for transfer from the cloud service provider in the event of termination of the services provided by the cloud service provider. If such period is determined by the cloud service provider, such entity would have an excessive broad margin to determine the term, which could potentially lead to unfair situations. In this sense, it is clear that customers would appreciate a time range for data porting.

- The IaaS Code of Conduct indicates that a cloud service provider may place limits on the scope of data it will transfer for a customer. There is a risk that such limits are inconsistent with the Article 6 Objectives.
- Both Codes of Conduct fail to ensure continuation of services during transfer from one cloud service provider to another. Without continuation of services being sufficiently addressed, it may lead to the very type of lock-in situation that the Codes of Conduct are intended to prevent.
- Both IaaS and SaaS Codes of Conduct permit the cloud service provider to unilaterally change the terms and conditions of data portability in circumstances where the customer would only have a termination right. This may lead to vendor lock-in and prohibit switching. It is suggested that at a minimum a clear statement be added to the Codes of Conduct that any such unilateral change must not undermine the Article 6 Objectives and that the cloud service provider must provide for a reasonably long period before the changes become effective so as to enable the customer to change to a new provider on the basis of the old terms.
- A cloud service provider may elect to comply with the IaaS and SaaS Code of Conduct in respect of some but not all of its IaaS services. It seems possible that the exercise of this discretion could: (i) adversely affect the ability of a customer to export data from the cloud service provider even where such data relates to a cloud service that adheres to the IaaS Code of Conduct; and (ii) enable misleading market practices and result in a lack of transparency (i.e. a customer may not understand that there is a difference between the "certified" and "uncertified" IaaS services provided by the cloud service provider). It may also lead to a lock-in situation in circumstances where the current cloud service provider adheres to the IaaS Code of Conduct in relation to that service but the purported new cloud service provider does not.
- With regard to the SaaS Code of Conduct also contains some leeway for CSPs especially with regard to security. The wording of the respective sections seems to imply that the CSP has a discretion as to whether to implement security measures and controls in connection with data export and data import. In our view, any such discretion would be inconsistent with the stated principle of the SaaS Code of Conduct (i.e. ease, efficiency and security of data portability for customers) and Article 6 Objectives.
- The SaaS Code of Conduct should make it clear that cloud service provider lock-in is not an acceptable business practice.
- The SaaS Code of Conduct does not adequately deal with access to data in the event of bankruptcy in line with Recital 31 of the Regulation. The SaaS Code of Conduct should include a reference to policies implemented and maintained by the cloud service provider that ensure the continuity of the service or, at least, the access to data in the event of bankruptcy.
- The SaaS Code of Conduct does not specify that it will be regularly reviewed and updated to keep pace with technological developments. Wording to this effect should

be added to the SaaS Code of Conduct in accordance with the recital 31 of the Regulation.

- We have also reviewed the SWIPO Common Governance and related documents, but these presented more limited concerns. One point of note relates to the declaration of adherence that must be made by a CSP. This declaration does not appear to be 'forward looking' and we wonder if it could be amended so as to require the CSP to also maintain its adherence to the relevant Code of Conduct so that such adherence is not fixed in time at the date of the declaration.

ANNEX 10: FURTHER DETAILS ON THE DESCRIPTION OF POLICY OPTIONS 2 AND 3

1. Overall design of the policy options

This Annex provides further details on the content of policy options 2 and 3, which are outlined in Chapter 5.

Each option is a realistic package of measures intended to address the general objective of increasing the value of data in the economy and society by ensuring that a wider range of stakeholders can control their data and that more data is available for use.

Each policy option combines several policy levers to address the specific objectives of the Data Act (which are detailed in Chapter 4), representing alternative emphases based on the input from stakeholders and analyses, namely:

In **B2B and B2C relations** (objectives 1 and 2):

- scope of rights and obligations regarding data;
- connected product design affecting how easily data can be accessed;
- conditions and compensation under which data is shared;
- promoting good commercial practice and addressing abuses of significant imbalances in businesses' bargaining power in contractual relationships;
- facilitating resolution of disputes.

In the **B2G context** (objective 3):

- obligation on businesses to make data available;
- obligations of accountability and transparency on public sector bodies in requesting and reusing the data.

For **cloud services** (objective 4):

- contractual and technical measures to enable switching in practice.
- obligation on cloud/edge service providers to take all reasonable measures to prevent unlawful access to data by non-EU/EEA authorities.

For **data interoperability** (objective 5)**:**

- standards for promoting interoperability.

2. Scope of the instrument in terms of the data covered

	Measure	**Type of data**	**Personal/non-personal data**
1	Empowerment of consumers and companies using connected products and related services	Data concerning the performance, use and environment of connected products and related services.	Personal (consumer) data and non-personal (industrial) data
2	Increasing availability of data for commercial use and innovation between businesses	Any kind of private sector data	Mostly non-personal (industrial) data, but some personal data is in scope.
3	Public sector reuse of commercially held data	Any kind of private sector data	Non-personal (anonymised or aggregated) data, exceptionally pseudonymised data

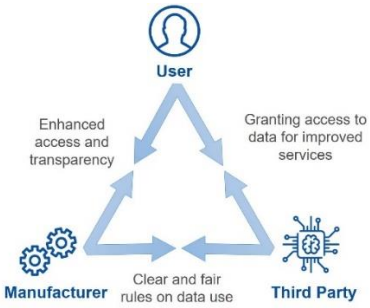
4	Switchability between cloud and edge services	Any kind of private or public sector data	Personal (consumer) data and non-personal (industrial) data

3. Policy Option 2 – Rules on controlled and predictable data sharing and reuse

Policy option 2 seeks to balance existing incentives to invest in data-generating activities with limited legislative measures that strengthen legal certainty on how data can be used and by whom, along with a general obligation to allow switching between cloud services.

PO2	***Objective 1: Empower consumers and companies using connected products and related services***

The relationship between user, manufacturer and third party under this option is illustrated below.



Measures:

- **Users' right to access data from their products**

Users, whether businesses or consumers, of a product would be granted the right to access, for free, the data that their connected product generates. This implies an obligation on the data holder to make such data available upon the request of the user.

If a user makes manifestly unfounded, excessive, or repetitive requests for the data, access may be refused or subject to a fee covering administrative costs.

- **Obligation on manufacturers to ensure that data from their products is easily accessible and transparency**

To enable the users' right, manufacturers would be obliged to ensure that data from their products is easily accessible to the user and to inform the customer, prior to purchase, what data are likely to be available.

A general transparency obligation of manufacturer vis-à-vis third parties as regards the kind of data that would be made available would allow such third parties to improve and innovate their services and to tailor them specifically to potential users and specific products.

- **Third party data access**

Users would be entitled to request from the data holder (which may be the manufacturer itself or another entity, e.g. a retailer that is able to give access to the data) to provide the data directly to a third party. Based on the analysis of the data transmitted, such third

parties may offer the user value added services, such as repair and maintenance. The data holder would be obliged to ensure easy access to such data by the third parties. However, the exact technical and practical arrangement of data access would be left to the data holder.

- **Manufacturer entitled to request compensation from third parties**

Where data is made available to a third party at the user's request, the manufacturer would be able to require compensation for making data available.

Manufacturers would be able to require compensation for making data available, based on a verifiable cost-based approach where the data recipient is an SME, and prevent discrimination between comparable categories of data recipients. In this case, cost for the SME would be limited to the cost of making the data available (reproduction and dissemination costs, such as costs of implementing APIs allowing continuous data access). Where the recipients are larger companies the parties would have the margin to negotiate a reasonable compensation. In such cases, large companies are considered capable of negotiating conditions and any compensation taking into account factors such as prevailing market conditions and return on investment. However, it should not lead to excessive prices that could have a discriminatory effect among larger companies.

The compensation rule is conceived as a maximum limit. Sectoral legislation could adopt less onerous pricing solutions (including free of charge access) where appropriate for specific sectors.

- **Machine-generated data excluded from Database Directive *sui generis* right**

Machine-generated data are a simple by-product of the main activity of a user of a connected product. These data have potential value for the development of innovative products and services, but this is hampered by legal uncertainty about exclusivity of rights to use the data. Policy option 2 would therefore explicitly exclude such data from the scope of application of the *sui generis* right under the Database Directive.

- **Small and micro manufacturers exempt from these new obligations**

Small companies, i.e. those that employ fewer than 50 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 10 million, would be exempted from the obligations to ensure easy access to data by users and third parties.

They would, however, remain subject to obligations to provide information and access to personal data in line with existing data protection rules.

- **Manufacturer's possibilities to use the data from products unaffected**

Manufacturer's existing possibilities to access and use data generated by their products would be unaffected, subject to data protection, competition, and other applicable rules.

Therefore, user empowerment would not result in an exclusive right on data or prevent the manufacturer, as an originator of the data, from continuing to exploit the data generated by the product and related services and from having a share in the generation of value downstream.

- **Existing data protection and electronic privacy rights and obligations unaffected**

For consumers using a product, this measure would complement Article 20 GDPR and extend to the non-personal data generated by the product. Data protection and privacy rights and obligations would otherwise be unaffected.

Any processing of data would be subject to compliance with applicable rules including the GDPR and Directive 2002/58/EC (ePrivacy Directive). Processing by a third party would require a separate legal basis, e.g. consent or contract with the consumer. Insofar as business' access and use of personal data generated by a product is concerned, such access and use would require a legal basis under the GDPR.

- **Existing sectoral data access rules unaffected but future convergence envisaged**

Existing sectoral legislation would be unaffected, but the Commission would aim to ensure full convergence with the Data Act when they are reviewed.

Any future sectoral rules may, within the framework of the Data Act, contain more detailed rules on eligibility of third parties, types of data to be made accessible, and technical access conditions which are appropriate for the sector.

PO2	***Objective 2: Increase availability of data for commercial use and innovation between businesses***

Measures:

- **Contractual unfairness test**

In addition to the voluntary model contract terms described under PO1, a contractual unfairness test for B2B data-sharing contracts, including co-generated data, would deprive unfair terms of their legal effect in order to protect the weaker party from excessive and abusive use of a strong imbalance of bargaining power in contractual relations. The unfairness test would target both parties to the contract, i.e. data holders as well as data requestors, in case either of them unilaterally imposes unfair terms on the other party. However, the scope of the unfairness test would be limited to protecting SMEs only as they are archetypically in a weaker bargaining position.

In terms of the main categories of contracts to be covered, the unfairness test would deal with data sharing contracts, contracts around products and services involving a data sharing element as well as contracts in the supply chain both in their downstream and upstream dimension.

The Data Act would lay down specific conditions to assess the potential unfairness of a contractual term. In this regard, the unfairness test would combine a list of clauses targeting specific clauses which are always unfair or are presumed to be with a general test of 'unfairness' (with criteria taken from existing EU *acquis*) catching those

remaining unfair clauses not covered by the lists, to ensure both legal certainty and effectiveness.

The unfairness test takes as a basis the principle of contractual freedom as an essential concept in B2B relationships. It does not aim at normal B2B contracts where parties negotiate a deal which is more favourable to the interests of the party with a stronger bargaining power. Its scope would instead be limited to contract terms unilaterally imposed on SMEs, i.e. 'take it or leave it' situations where the SME could not influence the terms of a contract. This requirement ensures that the unfairness test applies only in cases of a significant imbalance in negotiating power between the contracting parties.

The unfairness test only aims at the excessive use of such significant imbalance, which means that it leaves a very large freedom to parties to negotiate their contract clauses. In particular, the contracting parties would in any event be free to negotiate the price, unless determined in legislation. As competition law cannot solve the problem of contractual imbalances (the threshold of a dominant market position would not be reached in almost any of the cases at stake), an unfairness test would be the appropriate measure to tackle the abusive use of a strong imbalance in negotiating power (see Annex 11).

- **General rules for data access**

The rules applied to access to data generated by connected products and related services should also frame the rules around future, other data access obligations, in order to avoid the risk of fragmentation of data legislation and inconsistent approaches in the future.

In the case of future data access, the legislator would decide whether to grant such rights in sectoral legislation (regulating the 'if'), while the general access rules of the Data Act would set a general framework about the conditions which should apply to data access.

The Data Act would shape the general access rules in a concrete manner and therefore make the principles of fair, reasonable, transparent and non-discriminatory data sharing that are mentioned in the EU Strategy for Data and derived from existing EU legislation operational but without regulating the details of the contract.

Compensation

As in the case of data coming from connected products and related services, data holders would be able to require compensation for making data available, based on a verifiable cost-based approach and with a maximum level of charges is linked to the costs of making the data available where the data recipient is an SME. Where the recipient is a larger company, which due to a higher purchasing power does not need to be protected to the same extent as smaller companies, the appropriate level of compensation shall be left for the parties of the agreement to decide.

Non-discrimination

'Non-discriminatory' data access would mean that data access should be granted without discriminating between similarly situated data recipients. Data holders may treat recipients differently if this is justified. The reasons for different treatment however need to be objective. 'Transparency' is needed to put the requestor in a position to assess if the

above-mentioned conditions are met. There would also be limits to the transparency criteria, e.g. when third party intellectual property rights, trade secrets, the GDPR or confidential business information are concerned.

The general access rules are expected to also have the effect of spreading the use of these principles across sectors, i.e. even to those sectors where no sectoral data access rights have been created, influencing contractual practices, and thereby making fair and balanced data sharing contracts more widespread.

In general, based on the principle of contractual freedom, the parties would be free to negotiate the exact contractual conditions applicable in their case within the limits of the default access rules provided for in the Data Act and, where relevant, following the rules of the sectoral legislation creating a data access right or specifying how to access data. In this respect, the default access rules would be also linked to the rules of the unfairness test to ensure coherence.

- **Legal safeguards for data holders**

The Data Act would also include legal safeguards to protect data holders against misuse or misappropriation from data that was shared or obtained by another party, including in pre-contractual scenarios (i.e. where data is tentatively shared, before entering into a data transaction). The data recipient would be obliged to delete the data which were unlawfully obtained or misused and desist from their further exploitation.

- **Dispute resolution bodies**

The Data Act would ensure independent, impartial, transparent, effective, fast and fair dispute settlement bodies to be certified by Member States. These dispute settlement bodies would assist data holders and data requesters on a voluntary basis in finding an agreement when they face a dispute concerning the general access rules. Ensuring access to alternative ways of resolving domestic and cross-border disputes which arise in connection with making data available should benefit data holders and data requestors and therefore strengthen trust in data sharing. In cases where parties cannot agree fair, reasonable and non-discriminatory terms for making data available, dispute settlement bodies with expertise would offer a simple, fast and low-cost solution to data holders and data recipients. The Data Act would not prevent parties from exercising their right of access to the judicial system. The decision of the dispute settlement body shall only be binding if the parties have explicitly consented to its binding nature in advance.

.

PO2	***Objective 3: Introduce new mechanisms for the reuse of commercially-held data by public sector bodies in the case of exceptional need to use the data***

Measures:

Policy option 2 envisages a mechanism under the Data Act to enable public sector bodies to request and reuse data held by medium and large companies in exceptional situations.

The mechanism would complement existing reporting or compliance obligations in sectoral legislation that establish ongoing or recurring data exchange mechanism between public institutions and the private sector.

- **Exceptional needs**

Exceptional data needs include the need to respond to public emergencies and other situations where data is not otherwise available, for which the reuse of commercially held data is strictly necessary to enable public sector bodies to deliver more efficient public services and policies. This definition takes into account elements of the upcoming proposal for a Single Market Emergency Instrument.

The concept of 'public interest' is generally recognised in EU legislation, but there is no harmonised definition. Member States have a wide margin of discretion in defining the exact meaning of 'tasks carried out in the public interest' or the related concept of 'services of general economic interest'. Limiting the scope of B2G data sharing to exceptional situations makes the concept of 'public interest' as a requirement to determine what is covered less important. It is the exceptional character of the situation that will be the main criterion rather than the notion of 'public interest'.

'Public emergency' refers to exceptional situations negatively affecting a major part of a Member State(s) population or their fundamental rights, with a risk of serious and lasting repercussions on living conditions and the economic stability of the Member State(s). Public emergencies include major natural disasters and public health as well as human-induced major disasters, such as those caused by disruptions in production chains or terrorism.

Other exceptional situations should be clearly delimited to *ad hoc* needs and use-cases not covered by other mechanisms. Public sector bodies could request businesses' data when **conditions** a + b or a + c are met:

a) where the lack of available data prevents the public sector body or Union institution, agency or body from carrying out its core public tasks as defined by law or other binding rules of the Member States or of the Union

b) where the public sector body encounters exceptional difficulties in obtaining the data via existing mechanisms (e.g. procurement, buying the dataset from the provider, new and existing specific obligations in legislation cannot ensure the timely availability of data). These difficulties must be justified by objective reasons that make it impossible or very difficult to buy data on the market;

c) the use of B2G has a considerable potential to reduce the administrative burden for companies, in terms of replacing reporting obligations (e.g. replacing questionnaires with the use of scanner data in the field of statistics).

The burden of proof that conditions a-c apply would be on the public sector bodies that request the data.

- **Harmonisation and legal certainty**

The legislation would aim for maximum harmonisation in the interests of legal certainty for businesses and contain provisions preventing national law from expanding the scope of the Data Act by the Member States.

To ensure that the data obtained pursuant to the B2G rules of the Data Act do not enter the public domain and are used only to address the exceptional need justified in the request, the act would clarify that such data should not be considered open and should not be made re-usable. One exception to this rule might be accepted – that to share the data with a research institution, as long as the research activity is strictly linked to the original purpose for which the data was requested.

- **Exemptions**

Excluded from the B2G provision would be any requests for information for the purposes of law enforcement, judicial cooperation, taxation and customs or internal security. This is because legal obligations on B2G data use exist or will exist (e.g. passenger name records and anti-money laundering directives, the proposals on e-evidence and on strengthening. Europol's mandate) and data can in any case be obtained through standard judicial procedures.

A public sector body could use the expertise of public research institutes to analyse the data.

Given that most data is held by larger companies, in the interest of proportionality, small and micro companies would be exempt from the obligations of responding to requests – with the possibility of *ad hoc* exceptions where justified.

Finally, the Data Act provisions regulating access to private sector data would only apply to ad-hoc data requests in specific cases targeted (exceptional needs). They would be without prejudice to other EU and national rules on access to private sector data such as reporting obligations or obligations to provide information to ensure compliance.

- **Compensation and safeguards for businesses and citizens**

A compensation regime would apply whereby public sector bodies could be asked to cover (at most) the costs of data provision plus reasonable RoI to businesses for the use of the data[341]. In emergency situations, data would have to be provided for free. Specific conditions for compensation may be defined in sectoral legislation as long as they do not exceed the limits defined by the Data Act (this may include the possibility of a free of charge provision).

Safeguards would apply to ensure proportionality, transparency, respect for fundamental rights and freedoms, international trade rules and the rights and interests of the company

[341] European Commission (2022). *Outcome of the online consultation on the Data Act*;, only 15% of business respondents considered that the data should be provided at market price.

providing the data, as confirmed by public and private sector respondents to the consultation on this initiative[342].

- **'Once-only' principle**

As a principle, companies should not be asked for the same data for the same purpose more than once to avoid incurring excessive costs related to data provision. However, in cases where the costs of making the data available can be compensated and where companies can in addition claim a return on investment, there is no reason to prevent multiple requests.

A 'once-only' mechanism would therefore apply in cases where data needs to be provided free of charge, making it possible for companies to refer the public sector body asking for the same data to the other public sector body that has already received the data. This will avoid burdening companies with a duplicate request. This could be used as a 'defence mechanism' by the data holder who wishes to refuse the request for data in case it is repetitive.

- **Institutional mechanism for streamlining data requests and enforcement**

An institutional mechanism in each Member State (in the form of an appropriate competent authority to be appointed or established by the Member State) would ensure consistent application of the B2G provisions, provide a public register of requests, and facilitate the 'once-only' principle and cross-border cooperation. The same authority would be competent to enforce the provisions of the Data Act and to hear disputes between data holders and public sector bodies, including Union institutions and agencies.

- **Personal data protection and other rights**

In principle, anonymised data should be provided. In cases where personal data is strictly needed, it must be processed in compliance with the GDPR, the ePrivacy Directive or other relevant EU or national legislation. IP protection and trade secrets remain unaffected.

PO2	***Objective 4: Increase the trustworthiness and fairness of cloud and edge services***

Measures:

- **Legal obligation to facilitate switching**

Providers of cloud and edge services would be legally required to provide better framework conditions for switching on the basis of a set of minimum regulatory requirements regarding contractual aspects and applicable charges.

In this regard, examples of contractual aspects that would be covered as they have direct relevance for cloud switching are[343]:

[342] Ibid, 81% of public authority respondents considered transparent reporting on how the public authority has used the data to be necessary.

- The timeframes applicable to the completion of a switching process, measured from the moment of the user's notification of its intention to switch;
- The categories of (meta-)data included in the switching request;
- The inclusion of clear 'exit strategies' providing for data and application portability;
- A minimum period for data retrieval after the termination of a contract.

Additionally, this intervention would address the charges that cloud and edge providers impose on users during the switching process (e.g. data egress costs)[344].

In opposition to the Digital Markets Act, this approach would not present a direct portability obligation for concrete problematic services.

The technical aspects of interoperability of cloud and edge services would be addressed by a new approach based on enhanced standardisation (see section below).

- **Risks of potentially unlawful third country access**

To address concerns about potentially unlawful or unauthorised third-party access to cloud and edge, in line with Article 30 of the DGA (and using the formulation already endorsed by the Commission), providers would be required to take reasonable technical, legal, and organisational measures to prevent such access unless strict conditions are met. The safeguards would be intended to make unlawful data transfer without notification by the cloud service provider impossible, rather than resolving potential conflicts of laws with extraterritorially applicable laws of non-EU authorities.

The policy option would cover services offered on the EU market, rather than address (third country) data transfers or data flows. Such safeguards could include: periodic certification against a reputable standard, encryption for data at rest using external key management, anonymization/pseudonymisation technologies, split processing, and multi-party processing by independent providers[345].

The legislative intervention proposed under this policy option would not aim to affect the legal basis of access requests to data held by EU citizens or businesses and would be without prejudice to the EU's data protection and privacy framework.

- **Enforcement regime**

An appropriate enforcement regime, by building on existing capacities in the Member States' national regulatory authorities (NRAs). As most cloud services are offered in a majority of Member States, NRAs would need to cooperate at European level. This could be done by establishing an EU-level coordination group on cloud governance.

---

[343] European Commission (2018). *Switching of cloud services providers*, prepared by International Data Corporation (IDC) and Arthur's Legal, p. 37

[344] European Commission (2018). *Switching of cloud services providers*, prepared by International Data Corporation (IDC) and Arthur's Legal, p. 43

[345] European Commission (2022). Study to support an Impact Assessment on enhancing the use of data in Europe, prepared by Deloitte (Section 3.3.4).

PO2	*Objective 5: Establish a framework for efficient data interoperability*

Measures:

The option is designed to help ensure a minimal set of commonly agreed cross-sector and cross-border interoperability requirements and solutions, thus avoiding fragmentation and streamlining the interpretation of data within and across sectors and borders. The proposed measures are technologically neutral and future-proof, given that they would provide for a general fall-back competence of the Commission to recommend interoperability standards, which will be based on the assessment of the necessity and scope of such potential standards.

- **Non-binding criteria for technical means**

Policy option 2 would provide non-binding criteria for ensuring interoperability and respect for data sharing agreements between sectors through technical means, such as smart contracts and APIs.

- **Commission power to adopt common specifications**

In the absence of insufficient progress on interoperability, the Commission would be empowered to step in and adopt common specifications. Progress would be considered insufficient if:

1) a lack of open standards and interfaces constrains switching and innovation,
2) interoperability requirements or standards do not exist or are considered by the Commission to be insufficient, or specific concerns need to be addressed, and
3) the European standardisation system does not deliver sufficient progress.

The specifications would concern interoperability requirements and principles for facilitating data use in common European data spaces, data portability and interoperability between particular types of cloud and edge services.

- **Repository of cloud and edge interoperability standards**

The Commission would set-up a repository for cloud and edge interoperability standards to promote awareness and visibility of open standards and interfaces that technically enable switching of cloud and edge services, fully consistent with the forthcoming EU Cloud Rulebook[346].

- **Ensuring inclusivity in development of standards**

Under the Standardisation Regulation, the European Standardisation System is bound to respect the principles of inclusiveness and transparency. Its provisions ensure access of SMEs to standards and to the standardisation processes and oblige the Commission to consult the societal stakeholders and the organisations representing SMEs. This prevents

[346] As announced in the European Data Strategy, the Cloud Rulebook will offer a compendium of existing cloud codes of conduct and certification on security, energy efficiency, quality of service, data protection and data portability. It will be published by Q2, 2022.

the risk of large companies asserting their dominance and 'hijacking' the standardisation process.

4. Policy Option 3 – Rules for open data access between businesses and from businesses to public bodies

Policy option 3 proposes legislative measures to maximise the opportunities for parties to request access to data and determine how they can use it once available, with a wider range of companies entitled to reuse data held by businesses, and a regime for B2G which emulates the approach of G2B under the Open Data Directive.

PO3	***Objective 1: Empower consumers and companies using connected products and related services***

Measures:

- **User right to access data from their products**
- The user right to access data would foresee the same scope as in policy option 2. Specific technical requirements would apply. **Obligation on manufacturers to ensure that data from products are easily accessible to the user and transparency**

Manufacturers would be subject to the same obligations as under policy option 2.

- **Third party data access**

Users would be able to direct manufacturers to transmit data from their product or service directly to a third party.

Data holders would, in addition, be obliged to comply with common technical specifications, detailing how to enhance the possibility for providers of services to access the data. They would be required to apply technical means to enhance the possibility for providers of services, such as in aftermarkets, to access the data. Such technical requirements would be defined in terms of, for example, the necessary data latency, the API architecture, or minimum functionalities.

- **No entitlement to compensation from third parties**

Unlike policy option 2, there would be no right for manufacturers or service providers to require compensation for the cost incurred in making data available to a third party at the user's request.

PO3	***Objective 2: Increase availability of data for commercial use and innovation between businesses***

Measures:

- **Contractual unfairness test**

In addition to the measures under policy option 2, the unfairness test would apply to **all contractual terms** – not only unilaterally imposed terms – on data access and use, i.e.

also where the terms are not unilaterally imposed, but the other party was able to influence them.

- **Data misappropriation**

This option would not foresee additional legal safeguards to protect data holders against misappropriation of data. The Data Act itself would not foresee any possibility to restrict the data use for the data holder to protect his interests. With that, an even wider and less restrictive data use would be enabled.

PO3	***Objective 3: Introduce new mechanisms for the reuse of commercially-held data by public sector bodies***

Measures:

As under policy option 2, policy option 3 would set down general rules for conditions and compensation for public sector reuse of commercial data.

- **General mechanism for reuse of commercial data**

Public sector bodies would be able to request reuse of data beyond situations justified by an exceptional need for any duly justified purpose. Under this option, public sector bodies would have to explain the reasons for their data need, without proving exceptional circumstances such as the impossibility to obtain such data by available means or a substantive reduction of administrative burden. Such justification would be based on explaining e.g. how the data would facilitate to carry out the public tasks of the requesting public sector body.

- **Compensation**

Two levels of compensation for making data available would apply according to criteria for determining the urgency and importance of the circumstances of the request:

1) marginal cost for complying with the request for other purposes than public emergencies (e.g. urban planning, mobility, housing, and education);
2) free of charge in case of public emergencies (defined as under the EU solidarity mechanism).

- **Data stewards to facilitate B2G data sharing**

Public sector as well as medium and large companies would be required to designate a function ('data steward') responsible for handling public sector bodies' requests transparently and consistently[347].

This would reflect one of the main recommendations of the HLEG report.

PO3	***Objective 4: Increase the fluidity of the cloud/edge market and raise trust in***

[347] See Data Collaboratives *website*; and European Commission (2020). *Towards a European strategy on business-to-government data sharing for the public interest*, Final Report of the High-Level Expert Group on Business to Government Data Sharing.

	the integrity of cloud and edge servicess

Measures:

- **Detailed requirements on cloud switching**

Rather than setting the framework conditions, a broader and more specific legal provision than under policy option 2 would mandate direct switching and portability of cloud services. It would do so by presenting detailed requirements pertaining to interfaces, data semantics and architectures per each cloud service type: Infrastructure-as-a-Service (IaaS), Platforms-as-a-Service (PaaS), and Software-as-a-Service (SaaS).

Specify detailed parameters of switchability and binding interoperability requirements in the form, for example, of mandatory deployment of open interfaces and APIs.

- **Concerns about potentially unlawful access by third countries**

As under policy option 2, in line with Article 30 of the DGA, reasonable legal, technical, and organisational measures to address concerns about potentially unlawful access to data by non-EU/ EEA authorities.

PO3	***Objective 5: Establish a framework for efficient data interoperability***

Measures:

- **Commission power to adopt binding interoperability requirements**

The Commission would lay down in implementing acts data interoperability requirements facilitating data use in common European data spaces, for data portability and for interoperability between particular types of cloud and edge services. The requirements would be mandatory for all stakeholders.

ANNEX 11: THE UNFAIRNESS TEST IN THE DATA ACT

Unfairness test

The Impact Assessment uses the term 'unfairness test' in order to emphasise the fact that the objective of this test is not to define what is 'fair' in data sharing. It aims to deprive contract terms that are 'unfair', i.e. abusive, excessive contract terms, of their legal effect.

1. Unfairness test and freedom of contract

Following the objectives laid down in the Data Strategy, the unfairness test acknowledges the principle of contractual freedom as an essential concept in a B2B relationship at the stages of its scope and its application:

(1) First in terms of its scope, the unfairness test would be limited to protecting SMEs only, given that SMEs are archetypically in a weaker bargaining position. The unfairness test of the preferred policy option 2 would only apply in 'take-it-or-leave-it' situations where the contractual counterpart of the SME unilaterally imposes its contract terms, and the SME has not been able to influence their content despite the attempt to challenge them. This systemic limitation of its scope ensures that the unfairness test would only apply if there is a strong imbalance of bargaining power in the concrete contract at stake. A contract term that is simply provided by the contractual counterpart of the SME and accepted by the SME would not be considered as unilaterally imposed.

Furthermore, the scope of the unfairness test is also limited because it does not apply to the main subject matter of the contract or the price[348] to be paid. These are left to the parties' negotiations, unless the contract is based on a legal obligation to share data, which requires parties to follow the general rules on pricing in the Data Act.

Finally, while the unfairness test in the Data Act will look at contracts with a data sharing element, it will not apply to other parts of the same contract not related to data sharing.

(2) The second stage where contractual freedom is acknowledged is the application of the unfairness test itself. As a matter of principle, the contractual parties are free to negotiate the terms and conditions of the contract. Simply having a situation where one contractual party is able to obtain a better deal reflecting its stronger bargaining power does not mean that such contract terms are unfair. Therefore, the unfairness test does not concern clauses which are simply disadvantageous for one contractual party. Clauses which are to the advantage of one party and the disadvantageous to the other party are a normal part of contractual freedom, in particular in B2B contracts. The unfairness test looks thus at specific clauses of a contract to check whether they go beyond being simply disadvantageous and are abusive, putting an excessive burden on one party. Only such clauses are considered as an excessive use of a strong imbalance of bargaining power between the parties and consequently will be qualified as unfair and deprived of legal

[348] While the unfairness test applicable to voluntary data sharing will not look at the price, the general access rules applicable to mandatory data access will provide rules on compensation as well as establish a link to the unfairness test to ensure that mandatory data access is not unfair.

effect. The concluded contract, including clauses that are disadvantageous to one party, would, to the extent possible, remain valid without the unfair clauses.

2. Design and operation of the unfairness test

The design of the unfairness test should aim at reconciling legal certainty with effectiveness. Three main tools are available for an unfairness test:

- A general clause, which defines unfair clauses based on certain criteria. Such a clause and criteria are differently worded if they apply to B2C (e.g. in the Unfair Contract Terms Directive: 'contrary to the requirement of good faith, … a significant imbalance in the parties' rights and obligations arising under the contract, to the detriment of the consumer'[349]) or B2B (e.g. in the Late Payment Directive: a 'gross deviation from good commercial practice, contrary to good faith and fair dealing'[350]) and can be accompanied by considerations helping to apply them.

- A list, which contains clauses presumed to be unfair, depending on the circumstances of the case.

- A list of 'banned' clauses, which are considered unfair under all circumstances.

The list of banned clauses is the most legally certain, but it is the least effective tool as it is inflexible and vulnerable to circumvention. A general clause is, as such, not so legally certain because it is principle-based, but it is the most effective tool as it has the advantage of catching all remaining unfair clauses which are not yet covered by the lists.

A combination of a general clause with lists would capture all contract clauses and have a high degree of legal certainty as the lists cover the main categories of unfairness and serve to help the application of the general clause. The general definition of unfairness would borrow language from already established EU legislation, i.e. the criteria 'gross deviation from good commercial practice, contrary to good faith and fair dealing' (see above). The clauses in the lists would be derived from the study[351], based among others on discussions with stakeholders. Contractual problems and the corresponding solution provided for in the unfairness test would be, for instance:

Examples for problems[352]	**Solution**
Exclusion or limitation of remedies.	Included in the always unfair contract terms (if entirely excluded) and in the presumed unfair contract terms (where inappropriately limited).

[349] Article 3 of Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, OJ L 95 of 21.4.1993.
[350] Article 7 paragraph 1 of Directive 2011/7/EU on combating late payment in commercial transactions (recast), OJ L 48.1 of 23.2.2011.
[351] European Commission (2022, *forthcoming*). *Study on model contract terms and fairness control in data sharing and in cloud contracts and on data access rights*, prepared by ICF [section 6.2.2]
[352] European Commission (2022, *forthcoming*). *Study on model contract terms and fairness control in data sharing and in cloud contracts and on data access rights*, study prepared by ICF [section 6.2.2].

Exclusion or limitation of liability.	Included in the always unfair contract terms (for intentional acts or gross negligence and if entirely excluded) and in the presumed unfair contract terms (where inappropriately limited).
Excessive modalities of termination of a data sharing contract.	Included in the presumed unfair contract terms.
A contributor to generation of data not entitled to use the value of the contributed data.	Included in the presumed unfair contract terms.

The unfairness test would operate as follows (simplified):

- One party pre-drafts the contract terms and submits them to an SME. The SME tries to influence the content of one or several clauses, but the imposing party insists on them and says more or less that the contract will be concluded only if the relevant clauses are accepted, i.e. a 'take-it-or-leave-it' situation. The SME accepts the pre-drafted contract terms, as it does not want to lose the contract.

- The SME considers a particular contract term on data access and use, which it had previously tried to influence, as unfair, and contests it. As the other party insists on the term, the SME approaches the competent national court to decide the dispute.

- At first, the court will assess the scope, i.e. whether the contractual term was unilaterally imposed on the SME. If the party who supplied a contract term alleges that the term was not 'unilaterally imposed', that party should bear the burden of proving that this contract term was the result of negotiations with the SME or that the SME accepted that term without asking for changes. This could be relatively easily possible, for instance by submitting to the court the relevant e-mail exchanges between the parties.

- In general, the burden of proving that a clause is unfair is on the plaintiff. For assessing whether the contractual term is unfair, the court will in a first step check if the contract term in question forms part of the banned list of clauses. If not, the court will assess if it is included in the list of clauses that are presumed unfair. If yes, the contract term in question is considered unfair unless the party who unilaterally imposed the contractual term proves otherwise (rebuttable presumption). The party who unilaterally imposed the contractual term has the possibility to prove this because the clauses that are presumed unfair contain abstract legal terms which allow to interpret these clauses in the light of the particular circumstances of the contract at hand.

If the contract term in question is not included in the lists, the court will apply and interpret the general definition of unfairness ('grossly deviates from good commercial

practice in data access and use, contrary to good faith and fair dealing') and decide if the specific contract term is considered unfair. In this regard, the clauses enumerated in the lists serve as a benchmark to interpret the general clause. National default rules and the model contract terms for business-to-business data sharing contracts (to be developed by an Expert Group and recommended by the Commission) can also be useful in practice and will also give an indication if a contract term is not unfair.

- If the court comes to the conclusion that the contract term is unfair, the relevant contract terms is not binding on the SME. The other clauses of the contract, if the contract still works without that clause, continue to apply.

3. Unfairness tests in EU and Member States' legislation

A B2B contractual unfairness test is not a new, but an already familiar concept to EU and national laws.

EU legislation already includes rules on contractual fairness. Already in 1993, the Directive on Unfair Contract Terms introduced rules on contractual fairness in B2C contracts, which have been transposed and applied since long by all Member States.

Other EU legislative instruments also address fairness in B2B contractual relations for certain sectors or specific cross-cutting dimensions, notably the Late Payment Directive and the Directive on Unfair Trading Practices in the Agricultural and Food Supply Chain[353]. The aim of these Directives is to prevent unfair contractual practices while maintaining the principle of freedom of contract in relation to the commercial terms of the transactions. The two directives have a different approach to defining "unfair" contract terms. While the Late Payment Directive uses a general clause as explained in the previous section[354] as well as lists[355] of contractual clauses, the Directive on Unfair Trading Practices in the Agricultural and Food Supply Chain does not include a general clause but provides a list of specific prohibited trading practices in order to protect the interests of smaller suppliers of agricultural products who are presumed to have insufficient bargaining power when making transactions with powerful purchasers[356]. The benchmark of determining 'unfairness' in the Unfair Contract Terms Directive is lower than the Late Payment Directive and the Directive on Unfair Trading Practices in the Agricultural and Food Supply Chain as the former instrument aims to protect consumers which are in a situation of structural imbalance compared to the trader, while one can expect a higher degree of commercial diligence from businesses. These existing sectoral

[353] Directive (EU) 2019/633 on unfair trading practices in business-to-business relationships in the agricultural and food supply chain, OJ L 111/59 of 25.4.2019

[354] Article 7(1) stipulating that a contractual term or practice which excludes interest for late payment shall be considered as grossly unfair to the creditor should either be unenforceable, or give rise to a claim for damages

[355] Article 7(3) stipulates that a contractual term or practice which excludes compensation for recovery cost, shall be presumed to be grossly unfair.

[356] Article 3(1) provides black listed contractual terms, for instance, short notice cancellations of orders of perishable products, unilateral changes to agreed contract terms etc.

rules would continue to apply, while the unfairness test would apply to the data sharing elements of a contract. The rules in the Late Payment Directive and the Directive on Unfair Trading Practices in the Agricultural and Food Supply Chain do not concern specific data sharing elements and thus would not overlap with the unfairness test.

A slight majority of Member States have already established rules on unfair contract terms, which either do not distinguish in their application between B2C and B2B transactions or apply only in B2B contracts. These national unfairness tests consist generally of a general clause and/or specific listed clauses.

4. Interplay between a contractual unfairness test and the proposal for a DMA, competition law in general and the proposal for a DSA

Contract law, on the one hand, and the proposal for a DMA or EU competition law, on the other hand, represent two different areas of law with distinct angles, objectives, and tools. They deal with different situations. While competition law tackles market imbalances based on a dominant (or comparable) market position, contract law in the form of a contractual unfairness test would deal with imbalances in the specific contractual relationship and their possible excessive use. The Member States, which have rules on B2B fairness control (see above), also have separate rules on competition law.

By the same token, the purpose, scope and mechanism of the DMA and B2B unfairness test are also different. The DMA deals with situations of market imbalances where a party (the gatekeeper) has a strong market position. While the DMA has a very limited personal scope tackling large gatekeeper platforms, it reaches further on the substantive level establishing (positive) obligations to address unfair commercial practices.[357] On the contrary, a B2B unfairness test as regards data sharing has a broader personal scope dealing with contracts where a contractual party has a stronger negotiating power vis-s-vis an SME and unilaterally imposes unfair contractual terms. The party with a stronger negotiating position does not need to have – and generally does not have – a dominant (or comparable) market position or a gatekeeper position. The unfairness test addresses an abuse of an imbalance between contractual parties, not the market structure. However, on the substantial level the unfairness test is not that broad as the DMA. Firstly, it does not tackle commercial practices in general and does not contain any (positive) obligations. It only invalidates a specific contractual term on data access and use in a particular contract between the parties, if it is excessive or abusive. Also the general benchmark for the unfairness test expressed in the general clause (‘grossly deviates from good commercial practice in data access and use, contrary to good faith and fair dealing’) is formulated in a much narrower way than the benchmark for the Commission to supplement commercial practices considered unfair (‘where: (a) there is an imbalance of rights and obligations on business users and the gatekeeper is obtaining an advantage from business users that is disproportionate to the service provided by the gatekeeper to business users; or (b) the contestability of markets is weakened as a consequence of such a practice engaged in by gatekeepers’).

357

Finally, the DSA would not be concerned by the B2B unfairness test either. The DSA foresees among others transparency rules for terms and conditions stipulating that providers of intermediary services shall include information on any restrictions that they impose in relation to the use of their service in their terms and conditions. None of its provisions deal with unfair contract terms. There is no interference with the B2B unfairness test which tackles unfair contractual clauses on data access and use which are unilaterally imposed on SMEs. Purpose, scope and regulatory measures of the initiatives are entirely different.

5. Enforcement of the unfairness test and consistency in its application between the Member States

The enforcement of the unfairness will be left to Member States as done in any other EU contract law legislation. As a matter of principle, the EU contract law acquis does not create specific enforcement mechanisms, especially not in B2B transactions. Member States should be able to choose their usual enforcement mechanisms, i.e. courts or public authorities or both to enforce the rules. For cross-border disputes, Union law determines the applicable law and the competent court. EU law provides that parties to a B2B contract are free to choose the law governing the contract[358] and the competent court[359]. As at the moment slightly more than half of the Member States have rules on B2B unfairness control, this existing framework allows the contractual parties to circumvent the application of a B2B unfairness test by choosing a jurisdiction where such unfairness control is not foreseen. The harmonisation of the applicable standards through the unfairness test in the Data Act avoids this situation for data sharing contracts. As foreseen in the Treaty, consistency of interpretation will be ensured by the European Court of Justice, as it is done satisfactorily, for instance, in the context of the B2C unfairness test of the Unfair Contract Terms Directive.

6. Relation to model contract terms

Model contract terms and unfairness tests are two different, but complementary, instruments[360]. Their purposes and ways of achieving them are different. Model contract terms aim to influence in a positive way the design of a contract towards a fairer balance of contractual rights and obligations. The decision whether and to what extent they are integrated into the contract is left to the will of both contractual parties. The unfairness test, however, does not shape the design of the contract but aims at preventing excessive cases of unfair contractual practices through depriving such clauses of their validity.

[358] Article 3.1 of Regulation EC 593/2008 on the law applicable to contractual obligations.
[359] Regulation 1215/2012 on jurisdiction and recognition of judgements in civil and commercial matters.
[360] European Commission (2022, *forthcoming*). *Study on model contract terms, fairness test in B2B data sharing and cloud contracts and data access rights*, ICF, p. 69.