A first commentary to the proposal for a new Regulation on fair access and use of data (Data Act)*

Chiara Gallese

Abstract

The essay aims at examining the proposal for a new Regulation on fair access and use of data (Data Act), recently published by the European Commission. It examines the new legal framework in light of the European digital strategy, in particular the Strategy for Data, and describing how the proposal was conceived and inserted in the historical context. It also explores the newly introduced definitions, the scope of application, and the subjects of the proposal, identifying the most important legislative novelties and their consequences on different stakeholders. Lastly, it analyzes the normative gaps and the limitations of the current draft of the act.

Summary

Keywords

Data Act - European Digital Strategy - Digital Regulation - Data Access - Data Processing Services

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio "a doppio cieco". Funded by the REMIDE project, Carlo Cattaneo University - LIUC and by the UNI 4 JUSTICE Project

1. Introduction

The essay aims at examining the recent proposal for a new Regulation on fair access and use of data (Data Act), published by the European Commission on the 24th of February 2022. The proposal creates a new legal framework for the access and use of data, as depicted in Figure 1.

Firstly, we will focus on the European digital strategy, in particular the Strategy for Data, and on how the new proposal was conceived and inserted in the historical context. Secondly, we will explore the relevant definitions, scope of application, and subjects involved in the new legal framework. Thirdly, we will proceed to identify the most important legislative novelties introduced by the proposal and their consequences on different stakeholders. Lastly, we will examine the normative gaps left out of the proposal and the limitations of the current draft. Enacting this law will create new challenges and legal issues: to what legal cases will it be applicable? Who are the subjects that will be affected the most? What will be the consequences of the new legal framework? How is it harmonized with the existing legislation? What aspects is it failing to address?

We will answer these questions by analyzing the current text of the proposal, including the explanatory memorandum and the recitals, the related legislation (such as GDPR, which is complemented by this act), and the European Commission's working documents. We will also consider the current trends of the IoT market and the most common commercial practices in this field.

The analysis of the Data Act cannot be carried out only from a legal perspective, but business and technical point of views need to be taken into consideration as well, due to the fact that the object of the proposal is related to data generated by IoT devices, cloud computing and smart contacts are regulated, and interoperability requirements are a key element of the new legal framework.

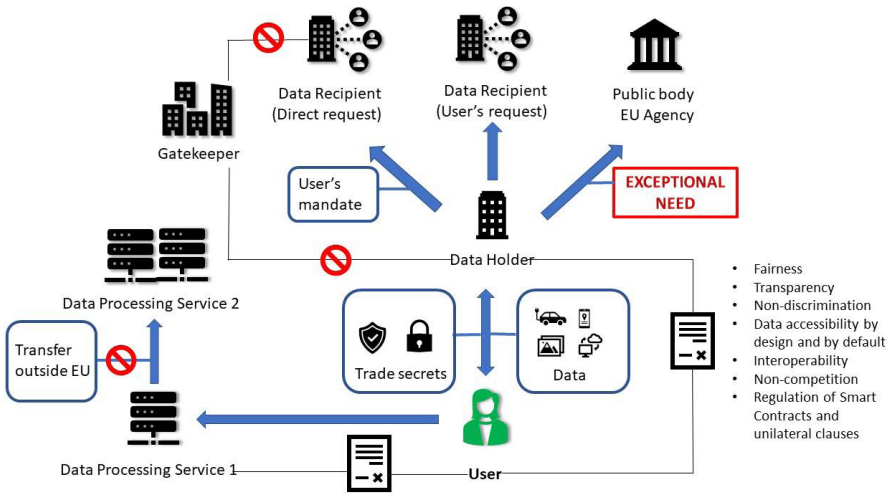

Figure 1: The framework of the Data Act

2. The European Digital Strategy and the background of the proposal

The proposal came into life as part of a broader European Digital Strategy regarding the movement of data in Europe. The interest of the EU in data, both from a perspective of protecting personal data and enhancing and harmonizing the sharing of data within the Union, began right after the Maastricht Treaty. As early as the 1995, the Database directive[1] was enacted, followed by the Data Protection Directive[2] the same year.

In 1997, with the development of the internet and the digital market, the EU started to regulate data protection in the telecommunications sector[3], and, in 2000, the field of electronic commerce[4]. 2002 has been a prolific year for the regulator, as five directives building the regulatory framework for electronic communications networks and services, together referred to as "the Framework Directive and the Specific Directives", were enacted[5].

In 2003, the Directive on the re-use of public sector information[6], now replaced by the Open Data Directive[7], was then enacted, following the desire of the European Commission to develop the potential of public sector data since the end of the 1980s[8].

In order to monitor the adoption, development and impact of electronic business practices, the European Commission launched the "e-Business W@tch" project in 2001. The project highlighted the need to create a suitable environment for companies

[1] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases.

[2] Directive 95/46/EC, now replaced by the 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 (GDPR).

[3] Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, replaced, in 2002, by the Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.

[4] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market.

[5] That is Directive 2002/19/EC of the European Parliament and of the Council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive), Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authorisation of electronic communications networks and services (Authorisation Directive), Directive 2002/21/EC of the European Parliament and the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive), Directive 2002/22/EC (Universal Service Directive), and the above mentioned Directive on privacy and electronic communications. They were regularly updated in the light of technological and market developments, e.g., by Directive 2006/24/EC and by Directive 2009/136/EC, but also sometimes temporarily derogated, e.g., by Regulation (EU) 2021/1232.

[6] Directive 2003/98/EC on the re-use of public sector information, known as the PSI Directive.

[7] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information.

[8] K. Janssen, *The influence of the PSI directive on open government data: An overview of recent developments*, in *Government Information Quarterly*, 28(4), 2011, 446 ss.

within the EU in order to ensure they are able to compete at a global level, including «cutting 'red tape', fostering innovation and – more specifically with regard to ICT – counteracting shortages in e-skills and promoting systems inter-operability»[9], as a response to the issues created by globalization and a growing international competition. These action points were included in the 2005 Action Plan and a new industrial policy was launched by the Commission in the same year.

In 2010, the Digital Agenda for Europe was announced as one of the seven flagship initiatives of the Europe 2020 Strategy. The aim was to create a digital single market, taking into consideration the need for interoperability[10], to tackle the fact that the EU was «falling behind in markets such as media services, both in terms of what consumers can access, and in terms of business models that can create jobs in Europe. Most of the recent successful internet businesses (such as Google, eBay, Amazon and Facebook) originate outside of Europe»[11].The European Commission was starting to wake up about the growing power of foreign giants, and since then it has finally being working to keep pace with international competitors. To enhance the digital market, the e-money Directive was created[12]. Key Directives supporting the digital single market, such as the Services Directive, Unfair Commercial Practices Directive, the Telecoms Framework, the e-Commerce Directive, the eSignature Directive, and the VAT Directive, contributed to the Digital Agenda.

In 2011, a comprehensive open data package was presented by the European Commission, following the route of the PSI Directive and working towards making available its documents in machine-readable format. In 2012, the EU Open Data Portal was launched, to promote the accessibility and reuse of information. The EU endorsed the G8 Open Data Charter in 2013, and committed to implementing open data activities.

The economic and financial crisis of 2008, the increasing surges of migrants and refugees, and the terrorist attacks starting in 2015, however, posed new challenges for the EU. Better communication across the Union become not only a goal to promote the single market and competitiveness[13], boosting and modernizing the economy, but also a crucial factor in fighting traditional and cyber terrorism, and other criminal acts[14]. The Directorate-General for Communication Networks, Content and Technology noted in 2012 that «in today's technological environment, any structural change must necessarily include a strong dose of digitisation. Europe's companies cannot remain

---

[9] European Commission, *The European e-Business Report 2006/07 edition - A portrait of e-business in 10 sectors of the EU economy - 5th Synthesis Report of the e-Business W@tch*, 2007.

[10] European Commission, *Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions - A Digital Agenda for Europe*, 2010; European Commission, *Digital agenda for Europe- Rebooting Europe's economy*, 2014.

[11] European Commission, *Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions - A Digital Agenda for Europe.*

[12] Directive 2009/110/EC on the taking up, pursuit and prudential supervision of the business of electronic money institution.

[13] European Commission, *Digital agenda for Europe- Rebooting Europe's economy.*

[14] European Parliament, *A new Digital Agenda for Europe: 2015.eu European Parliament resolution of 5 May 2010 on a new Digital Agenda for Europe*, 2010.

competitive, nor can public services remain first-class, if they do not make extensive use of information and communication technology (ICT). Virtually all newly created jobs require good ICT skills, and so do most existing jobs, too. Promoting ICT is promoting a job-rich recovery»[15].

The 2012 e-commerce action plan was aimed at doubling the volume of e-commerce in Europe by 2015 by optimizing postal delivery, enhancing electronic and mobile payments, promoting online shopping, improving Internet security and implementing measures to fight cyberattacks[16]. In 2014, the European Commission had completed 72 of 101 actions in the context of the Digital Agenda[17] and promoted the use of high-speed broadband «by bringing forward new rules on cost reduction, a recommendation on next generation access networks, revised state aid guidelines for broadband and a proposal to complete the telecoms single market»[18]. In the same years, the Commission started the works for a revision of the personal data protection regulatory framework, that were aimed at enacting the General Data Protection Regulation and the the ePrivacy Regulation.

However, despite these regulatory efforts, during the 2005-2015 decade the EU has not been able to defend its digital sovereignty from foreign Big Techs, which managed to enact a series of anti-competitive and tax-elusive practices, and to exploit personal data of European citizens. As noted by Gueham, «The time has come for a digital offensive – while the European Union resigned itself to American hegemony for several years, it never promoted the rise of a national champion capable of taking on Google or Amazon on equal terms, as China did with Alibaba or Russia with Yandex. The penalties imposed by Brussels on Microsoft and Intel for abuse of a dominant position stick in people's minds. Since 2010, and particularly since the new Commission took office in 2014, Europe has defied US imperialism, a permanent slight to its sovereignty, especially since the Snowden scandal which placed the spotlight on the US administration's use of European citizens' data. However, initiatives against American giants are still too rare to inspire fear»[19] . These circumstanced led the European Commission to focus its energies in defending fundamental rights against powerful foreign actors. In 2016-2018, in fact, GDPR largely transformed the privacy framework and posed the basis for an efficient defense of EU citizens'.

The data protection legislation reform that was initiated with GDPR was expanded in 2016 with the Law Enforcement Directive[20], applied from 2018.

In the same year the Regulation regarding the processing of personal data by the Un-

[15] European Commission, *Digital Agenda for Europe Scoreboard 2012*, 2012.

[16] European Commission, *Digital agenda for Europe- Rebooting Europe's economy*, 2014.

[17] *Ibid.*

[18] *Ibid.*

[19] F. Gueham, *Digital sovereignty – steps towards a new system of internet governance*, in *fondapol.org*, 2017.

[20] Directive 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

ion institutions[21], together with the Regulation regarding non-personal data[22], was enforced. This was the first seed that lead to the Data Act and the beginning of a novel regulatory effort aimed at enhancing the EU Digital Strategy.

In 2020, in fact, three other proposals were published: the proposal for a Regulation on contestable and fair markets in the digital sector (Digital Markets Act), the proposal for a Regulation on a Single Market for Digital Services (Digital Services Act)[23] and amending Directive 2000/31/EC, and the proposal for a Regulation on European data governance (Data Governance Act), which the Data Act complements.

Finally, in 2021, the proposal for a Regulation on Artificial Intelligence (AI Act) was published, providing strict rules regarding data sets employed in developing high-risk AI models.

The need for such an extensive regulatory framework has arisen since the volume of data produced in the world has increased from 33 zettabytes in 2018 to an expected 175 zettabytes in 2025[24]. The EU aims at becoming a leading role model by building «on a strong legal framework – in terms of data protection, fundamental rights, safety and cybersecurity – and its internal market with competitive companies of all sizes and varied industrial base»[25] .

In light of the above, it must be noted that big data is a crucial concept in the current era: processing such a large, complex and diverse amount of information enables data analysts to make accurate predictions in many areas and business sectors, such as health care, finance, marketing, and even environment, tackling major challenges, e.g., the climate change, as well as having a better understanding of social phenomena. It is also extremely important in the context of Artificial Intelligence, since machine learning models need a large amount of data to be trained[26]. It can be said, then, that a large part of the technological progress depends on the availability of data.

Having access to data is thus a powerful way to gain a business advantage over competitors. Because only large platforms now have access to a significant amount of data, there is a situation of oligopoly, in which the larger actors gain control over big data, and by analyzing it they are able to create more services and gain even more data, in a vicious circle. The European Commission pointed out that «The high degree of market power resulting from the 'data advantage' can enable large players to set the rules on the platform and unilaterally impose conditions for access and use of data

[21] Regulation 2018/1725 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data.

[22] 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.

[23] G. De Minico, *Fundamental rights, European digital regulation and algorithmic challenge*, in *Rivista di diritto dei media*, 1, 2021, 9 ss.

[24] European Commission, *Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions - A European Strategy For Data*, 2020.

[25] *Ibid.*

[26] Regarding the use of data to train AI models, the new proposal for a Regulation on Artificial Intelligence (AI Act) has drawn a new framework with the aim of removing biases in data sets whenever the system is considered as "high risk".

or, indeed, allow leveraging of such 'power advantage' when developing new services and expanding towards new markets. Imbalances may also arise in other situations, such as with regard to access to co-generated IoT data from industrial and consumer devices»[27].

Of all this data, a research from International Data Corporation (IDC 2019) has estimated that a large part (79.4 zettabytes) will be generated by connected devices (IoT) by 2025. Those devices will then become more and more important in the data economy. However, because the data generated by them are hosted in proprietary platforms and cloud solutions, only the producers have access to that information. The proposal of the Data Act aims at changing this situation by giving control back to users, who are the subjects of the data generating process, by rebalancing the contractual power for SMEs through the provision of fair clauses in data sharing contracts, and by allowing public sector bodies to access and use data held by private companies in exceptional circumstances.

The background of the new regulation is well explained in Recital 1 and 2, which explain that, while the digitization of economy is growing and electronic data are valuable elements of new technologies[28], data processing activities are hindered by data localization requirements and lock-in practices[29]. To exploit the data value chains of IoT systems and to cope with new legal issues[30], a legislative intervention has been necessary.

In addition, the Data Act reviews part of the Database Directive, in order to prevent the copyright protection of IoT data which could be used as an excuse to limit the right of access: «In order not to hinder the exercise of the right of users to access and use such data in accordance with Article 4 of this Regulation or of the right to share such data with third parties in accordance with Article 5 of this Regulation, the sui generis right provided for in Article 7 of Directive 96/9/EC does not apply to

[27] European Commission, *Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions - A European Strategy For Data*, cit.

[28] Recital 1: «The digitisation of the economy is accelerating. Information and Communications Technology is no longer a specific sector, but the foundation of all modern innovative economic systems and societies. Electronic data are at the centre of those systems and can generate great value when analysed or combined with services and products».

[29] Recital 2: «Data value chains are built on different data activities: data creation and collection; data aggregation and organisation; data processing; data analysis, marketing and distribution; use and re-use of data. The effective and efficient functioning of data processing is a fundamental building block in any data value chain. However, the effective and efficient functioning of data processing, and the development of the data economy in the Union, are hampered, in particular, by two types of obstacles to data mobility and to the internal market: data localisation requirements put in place by Member States' authorities and vendor lock-in practices in the private sector».

[30] As noted by the second part of Recital 1: «At the same time, the rapid development of the data economy and emerging technologies such as Artificial Intelligence, Internet of Things products and services, autonomous systems, and 5G are raising novel legal issues surrounding questions of access to and reuse of data, liability, ethics and solidarity. Work should be considered on the issue of liability, in particular through the implementation of selfregulatory codes and other best practices, taking into account recommendations, decisions and actions taken without human interaction along the entire value chain of data processing. Such work might also include appropriate mechanisms for determining liability, for transferring responsibility among cooperating services, for insurance and for auditing».

databases containing data obtained from or generated by the use of a product or a related service».

3. Scope of application, definitions, and subjects of the Data Act

Article 1 of the proposal defines its scope of application and subject matter: it is aimed at harmonizing the rules about data generated by the use of "a product or related service", in order to make it available from "data holders" to:
the User (natural or legal person who generates the data);
Data Recipients (natural or legal person who receives the data in the context of their business or professional activity);
public sector bodies or Union institutions, agencies or bodies, in case of exceptional need and for the performance of a task carried out in the public interest.
The definition of the term "data"[31] is borrowed from the Data Governance Act: «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 audio-visual recording». Although it is rather broad, its relevance is specified by the definition of "product", i.e. «a tangible, movable item, including where incorporated in an immovable item, that obtains, generates or collects, data concerning its use or environment, and that is able to communicate data via a publicly available electronic communications service and whose primary function is not the storing and processing of data» and by that of "related service", that is a «digital service, including software, which is incorporated in or inter-connected with a product in such a way that its absence would prevent the product from performing one of its functions».
In this context, it is clear that the proposal intends to restrict the definition to data generated by all connected devices[32], including robots, with the exception of those devices that have a mere accessory function (such as hard drives, dock stations, decoders, modems, WiFi bridges, etc.). Interestingly, Recital 15 excludes some of the most common IoT devices: «Certain products that are primarily designed to display or play content, or to record and transmit content, amongst others for the use by an online service should not be covered by this Regulation. Such products include, for example, personal computers, servers, tablets and smart phones, cameras, webcams, sound recording systems and text scanners. They require human input to produce var-

[31] While the OECD defines it as «data can be described as the unordered and unprocessed representation of any types of observations that are quantified and stored in symbols» in *Introduction to Data and Analytics (Module 1): Taxonomy, Data Governance Issues, and Implications for further Work*, OECD 2013.

[32] Recital 14 makes reference to IoT devices: «Physical products that obtain, generate or collect, by means of their components, data concerning their performance, use or environment and that are able to communicate that data via a publicly available electronic communications service (often referred to as the Internet of Things) should be covered by this Regulation. Electronic communications services include land-based telephone networks, television cable networks, satellite-based networks and near-field communication networks. Such products may include vehicles, home equipment and consumer goods, medical and health devices or agricultural and industrial machinery».

ious forms of content, such as text documents, sound files, video files, games, digital maps». The exclusion of smart phones, tablets, notebooks, and cameras, which are known to generate a large amount of data and metadata of great value, significantly reduces the scope of this proposal. For example, smart phones are commonly used as tools for delivering tele-health services[33], to control other IoT devices,[34] etc. Modern smarthpones are not just telephones anymore, they can become specific devices through mobile apps (e.g., controlling heating, lighting, and doors of the house). In many cases, there is little difference between a smartphone and a different IoT device, therefore this exclusion seems incongruous.

On the other hand, the definition is to some degree extended by the inclusion of data generated by digital services, such as proprietary software running in IoT devices. It is unclear, however, what software is exactly included in the definition of "digital service". The article specifies that a piece of software is included if «its absence would prevent the product from performing one of its functions», but it does not define what is a "function". For example, are third-parties proprietary apps such as Google Maps, installed on smart devices, included? One of the function of modern IoT devices (e.g., smart watches) is to enable their owner to navigate on the web, use social media, send messages, make calls through internet, take pictures, etc. Some of them have built-in and pre-installed apps, which cannot be uninstalled by the User.

Article 7[35] further extend the concept to "virtual assistants", defined as «software that can process demands, tasks or questions including based on audio, written input, gestures or motions, and based on those demands, tasks or questions provides access their own and third party services or control their own and third party devices». The reference is clearly to popular systems such as Siri, Alexa, and Google Assistant, which are used by millions of people worldwide, for example to search for information, control smart devices in the house, listen to music, do shopping, etc.[36]

Recital 22 contains an explanation about the scope of the Regulation regarding virtual assistants and it also gives a hint about the relevance of apps: «Virtual assistants play an increasing role in digitising consumer environments and serve as an easy-to-use interface to play content, obtain information, or activate physical objects connected to the Internet of Things. Virtual assistants can act as a single gateway in, for example, a smart home environment and record significant amounts of relevant data on how users interact with products connected to the Internet of Things, including those manufactured by other parties and can replace the use of manufacturer-provided in-

[33] S. D. Burdette – T. E. Herchline – R. Oehler, *Practicing medicine in a technological age: using smartphones in clinical practice*, in *Clinical infectious diseases*, 47(1), 2008, 117 ss.; D.C. Baumgart, *Smartphones in clinical practice, medical education, and research*, in *Archives of internal medicine*, 171(14), 2011, 1294 ss.; W. J. Gordon et al., *Beyond validation: getting health apps into clinical practice*, in *NPJ digital medicine*, 3(1), 2020, 1 ss.

[34] X. Mao et al., *Design and implementation of a new smart home control system based on internet of things*,. in *2017 international smart cities conference (ISC2)*, IEEE, 2017, 1 ss.

[35] «Where this Regulation refers to products or related services, such reference shall also be understood to include virtual assistants, insofar as they are used to access or control a product or related service».

[36] M. B. Hoy, *Alexa, Siri, Cortana, and more: an introduction to voice assistants*, in *Medical reference services quarterly*, 37(1), 2018, 81 ss.; I. Lopatovska et al., *Talk to me: Exploring user interactions with the Amazon Alexa*, in *Journal of Librarianship and Information Science*, 51(4), 2019, 984 ss.

terfaces such as touchscreens or smart phone apps. The user may wish to make available such data with third party manufacturers and enable novel smart home services. Such virtual assistants should be covered by the data access right provided for in this Regulation also regarding data recorded before the virtual assistant's activation by the wake word and data generated when a user interacts with a product via a virtual assistant provided by an entity other than the manufacturer of the product. However, only the data stemming from the interaction between the user and product through the virtual assistant falls within the scope of this Regulation. Data produced by the virtual assistant unrelated to the use of a product is not the object of this Regulation». Data gathered from apps seems thus included in the scope of the regulation insofar they are related to the interaction between the User and the product.

In addition, Recital 16 makes reference to software as a service (SaS), including in the scope also third-party services which are part of the original contract: «Such related services can be part of the sale, rent or lease agreement, or such services are normally provided for products of the same type and the user could reasonably expect them to be provided given the nature of the product and taking into account any public statement made by or on behalf of the seller, renter, lessor or other persons in previous links of the chain of transactions, including the manufacturer. These related services may themselves generate data of value to the user independently of the data collection capabilities of the product with which they are interconnected. This Regulation should also apply to a related service that is not supplied by the seller, renter or lessor itself, but is supplied, under the sales, rental or lease contract, by a third party. In the event of doubt as to whether the supply of service forms part of the sale, rent or lease contract, this Regulation should apply». Therefore, third-parties apps may be included in the definition of "related services", although it seems that not all data generated by those apps are subject to the Data Act.

In fact, Recital 17 clarifies that Users' recordings that were made on purpose are within the scope of the Regulation, together with data generated by Users' actions: «Data generated by the use of a product or related service include data recorded intentionally by the user. Such data include also data generated as a by-product of the user's action, such as diagnostics data, and without any action by the user, such as when the product is in 'standby mode', and data recorded during periods when the product is switched off. Such data should include data in the form and format in which they are generated by the product, but not pertain to data resulting from any software process that calculates derivative data from such data as such software process may be subject to intellectual property rights», while Recital 14 excludes the results of data analysis from the scope of the proposal[37].

[37] «The data represent the digitalisation of user actions and events and should accordingly be accessible to the user, while information derived or inferred from this data, where lawfully held, should not be considered within scope of this Regulation».

3.1 Subjects of the proposal

After defining the relevant terms, the subjects to whom the proposal is aimed are identified:

- manufacturers of products and suppliers of related services and their users in the European market;
- Data Holders that make data available to Data Recipients located in the Union, and to public sector bodies and Union institutions, agencies or bodies;
- Data Recipients located in the Union;
- Data Holders that provide data in cases of exceptional need;
- Providers of Data Processing Services (DPS) targeting customers in the Union.

The focus of the proposal is to extend the legal protection to all products that are available to European consumers, regardless of the subject who is putting them into the market. In this way, foreign companies targeting EU customers need to comply as well.

However, Article 7 restrict the scope of the proposal to medium and big enterprises, explicitly excluding micro and small enterprises[38], provided that they are not partnered or linked to larger enterprises[39]. This provision intends to avoid to impose additional burdens to companies that have lesser means to comply, while at the same time preventing bigger companies to circumvent the regulation by establishing smaller new branches or controlled entities.

Three subjects are introduced by this provision, namely the "Data Holder", the "Data Recipient", and the "User". The first one can be considered the equivalent of the "Data Controller" in GDPR, while the last one is correspondent to the "Data Subject", although it is not restricted to natural person, but it includes legal persons as well. The Data Recipient, which is sometimes referred to as "Third Party", on the other hand, corresponds to the "Third Party" concept in GDPR (including Data Processors).

3.2 Relationship with GDPR

The concept of data is not restricted to non-personal data, although personal data are already covered by GDPR, which prevails over the provisions of the Data Act[40].

The novelty of this proposal is that it covers also *anonymized data*, that is, information that was originally classified as personal data, but then put through a number of technical operations to remove the elements that could lead back to identification of the data subject. In doing so, the legislator intends to regulate and curb the habit of large

[38] As defined in Article 2 of the Annex to Recommendation 2003/361/EC: less than 50 employees and a turnover and/or balance sheet that does not exceed 10 million EUR.

[39] Also as defined in Article 3 of the Annex to Recommendation 2003/361/EC.

[40] In fact, the regulation itself reminds multiple times that GDPR should be respected: «Where the user is not a data subject, any personal data generated by the use of a product or related service shall only be made available where there is a valid legal basis under Article 6(1) of Regulation (EU) 2016/679 and where relevant, the conditions of Article 9 of Regulation (EU) 2016/679 are fulfilled».

companies to take advantage of users' personal data by claiming that they were "fully anonymized"[41] and thus not subject to GDPR obligations, such as the right of access and right to portability.

Personal data protection interrelates with the Data Act when Users' data are personal data or the data set is mixed (personal and non personal data). In fact, in this case Data Holders are also Data Controllers and Users are Data Subjects (see Recital 24), and all GDPR provisions must be respected (see Recital 30), including the rights of access and portability. This proposal confer to Data Subjects the right to receive not only their personal data, but also non personal ones.

The data portability right is, in fact, expanded by the proposal, providing that data generated by the use of a product or related service can be made available to a third party at the request of the user.

While Article 20 provides for a right of Data Subjects to receive the personal data they provided to the Data Controller «in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided», when the legal basis for the processing is consent or a contract and it is carried out by automated means. According to the same article, in addition, Data Subjects have the right to «have the personal data transmitted directly from one controller to another, where technically feasible» This right does not apply to «processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller».

Recital 31 notes that «Article 20 specifies that it pertains to data provided by the data subject but does not specify whether this necessitates active behaviour on the side of the data subject or whether it also applies to situations where a product or related service by its design observes the behaviour of a data subject or other information in relation to a data subject in a passive manner». The wording of the article is not dirimment at this regard, but it seems to suggest at least the will to share the data.

Recital 31 further specifies that the Data Act intends to complement the right to portability, but in a broader way, as it «grants users the right to access and make available to a third party to any data generated by the use of a product or related service, irrespective of its nature as personal data, of the distinction between actively provided or passively observed data, and irrespective of the legal basis of processing. Unlike the technical obligations provided for in Article 20 of Regulation (EU) 2016/679, this Regulation mandates and ensures the technical feasibility of third party access for all types of data coming within its scope, whether personal or non-personal. It also allows the data holder to set reasonable compensation to be met by third parties, but not by the user, for any cost incurred in providing direct access to the data generated by the user's product. If a data holder and third party are unable to agree terms for such direct access, the data subject should be in no way prevented from exercising the rights contained in Regulation (EU) 2016/679». Therefore, it is explained that the right enshrined in GDPR prevails over that contained in the Data Act.

[41] Very often, the process of anonymization is not even carried out according to the Working Party 29's Opinion on Anonymization Techniques of 2014.

Users may also be Data Controllers themselves, for example in the case of IoT devices used by employees of a company. By filing a data access request, the company may acquire its employees' (or a different person's) personal data, becoming a Controller. When Users assume the role of Controllers, they must have a valid legal basis according to GDPR for requesting personal data generated by the use of a product or related service. For example, in case of a company wanting to get access to their employees data, a legitimate interest might be present. Clearly, in this case the User-Controller must ensure that the Data Subjects concerned are informed pursuant to Article 14 of GDPR.

It might also happen that the Data Holder and the User are qualified as Joint Controllers, pursuant to Article 26 of GDPR. In this case, a contractual agreement is needed to determine their respective responsibilities, in particular as regards the exercising of the rights of the data subject and in providing the privacy notices according to Articles 13 and 14.

As highlighted by Recital 30, once data has been made available, the User might as well become a Data Holder, thus acquiring the obligations to make data available under the Data Act.

4. Data accessibility by design and by default and the right of access

Article 3 introduces for the first time a principle of "data accessibility by design and by default", meaning that systems need to be designed and set in such a way that Users can easily - and, if possible, directly - have access to the information generated by the device[42]. The provision is complementing the right of access enshrined in GDPR.

The main novelty of the regulation is in fact the provision of the right of access to users' data, contained in the first paragraph of Article 4: «Where data cannot be directly accessed by the user from the product, the data holder shall make available to the user the data generated by its use of a product or related service without undue delay, free of charge and, where applicable, continuously and in real-time. This shall be done on the basis of a simple request through electronic means where technically feasible».

[42] In fact, the Article states the following: «Products shall be designed and manufactured, and related services shall be provided, in such a manner that data generated by their use are, by default, easily, securely and, where relevant and appropriate, directly accessible to the user», and recital 20 further specifies that «In case several persons or entities own a product or are party to a lease or rent agreement and benefit from access to a related service, reasonable efforts should be made in the design of the product or related service or the relevant interface so that all persons can have access to data they generate. Users of products that generate data typically require a user account to be set up. This allows for identification of the user by the manufacturer as well as a means to communicate to exercise and process data access requests. Manufacturers or designers of a product that is typically used by several persons should put in place the necessary mechanism that allow separate user accounts for individual persons, where relevant, or the possibility for several persons to use the same user account. Access should be granted to the user upon simple request mechanisms granting automatic execution, not requiring examination or clearance by the manufacturer or data holder. This means that data should only be made available when the user actually wants this. Where automated execution of the data access request is not possible, for instance, via a user account or accompanying mobile application provided with the product or service, the manufacturer should inform the user how the data may be accessed».

The key concept of this provision is that all data generated by an IoT system, which is not already in the control of the User, can now be accessed by the same User at no cost and without undue delay. This means that, whenever the data generated by the system is not under the direct control of the User and it is not possible to download it directly, the User has the right to receive a copy and is now able to process it independently from the Data Holder.

Some example of data that can be requested are, for example, travel routes, gasoline consumption, speed fluctuation, breaking and accelerating frequency, travel time and frequency, tire pressure, motor oil level and consumption, maintenance frequency, regarding a connected car; time of switching on and off, duration, frequency of usage, and intensity levels of a smart light bulb; usage, charge and status of battery, time of switching on and off and connection to the internet, maintenance data, related to smart glasses.

The proposal puts an accent on the benefits of this provision for individuals and companies, especially because of the fact that it will allow them to switch to a different enterprise to perform maintenance activities. In fact, a common problem is that many IoT products (e.g., cars, industrial machinery) can be repaired and updated only by their producers or by authorized retailers, as the relevant data, that would allow to understand how the system works, is not disclosed by the manufacturer. Producers often hide under the "trade secret" excuse, claiming that disclosing maintenance data would imply sharing protected information. The proposal puts a full stop to this practice.

In fact, regarding trade secrets[43], the proposal prescribes at par. 3 of Article 4 a legitimate basis for the disclosure according to article 3, par 1, lett. d), of the Trade Secret Directive, but it imposes a condition to be fulfilled: it is possible to request the disclosure of trade secrets «provided that all specific necessary measures are taken to preserve the confidentiality of trade secrets in particular with respect to third parties». Those measures can be agreed between the Data Holder and the User. However, par. 6 of Article 8 provides that this regulation does not impose an obligation to disclose such information [44]. Therefore, although producers are now obliged to share the relevant data, they can do it without disclosing trade secrets, and they cannot hide the data claiming that it constitutes a secret. As an additional reassurance for Data Holders, a non-compete provision has been inserted to prevent unfair use of data obtained thanks to this regulation, providing that «The user shall not use the data obtained pursuant to a request referred to in paragraph 1 to develop a product that competes with the product from which the data originate».

This provision is counterbalanced by paragraph 6, which set a symmetrical limit to the use of data generated by the User: «The data holder shall only use any non-personal data generated by the use of a product or related service on the basis of a contractual agreement with the user. The data holder shall not use such data generated by the

[43] The concept is defined by the Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (Trade Secret Directive).

[44] «Unless otherwise provided by Union law, including Article 6 of this Regulation, or by national legislation implementing Union law, an obligation to make data available to a data recipient shall not oblige the disclosure of trade secrets within the meaning of Directive (EU) 2016/943».

use of the product or related service to derive insights about the economic situation, assets and production methods of or the use by the user that could undermine the commercial position of the user in the markets in which the user is active».

On one hand, then, the User cannot exploit the data to become a competitor of the Data Holder, as this would be an unfair practice and the proposal intend to prevent the right of access to be used as an excuse to steal trade secrets and business information to gain a commercial advantage. On the other hand, paragraph 6 conversely makes sure that data generated by the User is regulated by a contract between the two parties, and prevents the Data Holder to exploit the User's data in an unfair way that would undermine the User's position in the market. This is also to prevent larger companies to exploit data obtained by SMEs.

The introduction of the right of access will have an impact on both large companies and SMEs, as well as on citizens. Natural persons will be able to have a better insight on data they generate, being able to analyze it and having a more complete picture of their IoT systems, for example by learning what profile has been built, what preferences are tracked by the Data Holder, enabling them to make informed choices regarding consent and device settings. They will also be able to transfer the data into different systems and to store them as they prefer. This will facilitate maintenance operations, as they will be able to provide to repair services all relevant information. The difference with the right of access pursuant to GDPR is that Users are now able to obtain also the information derived from personal data, which previously was excluded because it was classified as anonymized data, and which enables non-SME enterprises to sell data to advertisers without complying to GDPR.

SMEs will benefit even more from this provision, as they will be able to analyze their own data to perform gap analysis and improve their internal procedures and products (e.g., in the transportation industry, by improving management of trucks and travel route, monitoring compliance with road rules, improving shifts of drivers). According to McKinsey, through the analysis of IoT data for predictive maintenance, maintenance costs and equipment downtime can be significantly reduced, and in the factories setting, it is possible to achieve a «10 to 20 percent energy savings and a 10 to 25 percent potential improvement in labor efficiency»[45].

However, there are still some obstacles to the possibility of data exploitation. One is the fact that in some sectors there is an oligopoly of manufacturers, so that Users have difficulties in finding alternatives and their control over the data is limited[46]. To overcome part of this issue, the proposal tries to empower Users by giving a better control over their data and by providing non-competition obligation, preventing Data

[45] McKinsey Global Institute, *The Internet of Things: Mapping the value beyond the hype,* in *mckinsey.com*, June 2015.

[46] Recital 25 highlights this problem: «In sectors characterised by the concentration of a small number of manufacturers supplying end users, there are only limited options available to users with regard to sharing data with those manufacturers. In such circumstances, contractual agreements may be insufficient to achieve the objective of user empowerment. The data tends to remain under the control of the manufacturers, making it difficult for users to obtain value from the data generated by the equipment they purchase or lease. Consequently, there is limited potential for innovative smaller businesses to offer data-based solutions in a competitive manner and for a diverse data economy in Europe».

Holders to exploit the data to undermine the economic position of the User on the market[47]. Recital 25 also suggests to rely on sectoral legislation and Codes of Conduct[48], as its 2018 predecessor Regulation regarding Non-Personal Data[49].
Another issue is the fact that lock-in practices are still very common, and not every data is shared. Manufacturers often retain their data sets in proprietary format, so that it is impossible to port them in a different environment[50].
For this reason, the proposal introduced the right of Data Portability and some interoperability requirements, excluding micro and small enterprises by the envisaged obligations[51].

5. Data Portability, Fairness, Reasonableness, and Non-discrimination

Article 5 provides for the "Right to share data with third parties", that is, the Data Portability principle: «Upon request by a user, or by a party acting on behalf of a user, the data holder shall make available the data generated by the use of a product or related service to a third party, without undue delay, free of charge to the user, of the

[47] Recital 25 reminds that « [...] the data holder should not use any data generated by the use of the product or related service in order to derive insights about the economic situation of the user or its assets or production methods or the use in any other way that could undermine the commercial position of the user on the markets it is active on. This would, for instance, involve using knowledge about the overall performance of a business or a farm in contractual negotiations with the user on potential acquisition of the user's products or agricultural produce to the user's detriment, or for instance, using such information to feed in larger databases on certain markets in the aggregate (e.g. databases on crop yields for the upcoming harvesting season) as such use could affect the user negatively in an indirect manner. The user should be given the necessary technical interface to manage permissions, preferably with granular permission options (such as "allow once" or "allow while using this app or service"), including the option to withdraw permission».

[48] «This Regulation should therefore build on recent developments in specific sectors, such as the Code of Conduct on agricultural data sharing by contractual agreement. Sectoral legislation may be brought forward to address sector-specific needs and objectives».

[49] At Article 6: «The Commission shall encourage and facilitate the development of self-regulatory codes of conduct at Union level ('codes of conduct'), in order to contribute to a competitive data economy, based on the principles of transparency and interoperability and taking due account of open standards [...]».

[50] Recital 19 notes that «In practice, not all data generated by products or related services are easily accessible to their users, and there are often limited possibilities for the portability of data generated by products connected to the Internet of Things. Users are unable to obtain data necessary to make use of providers of repair and other services, and businesses are unable to launch innovative, more efficient and convenient services. In many sectors, manufacturers are often able to determine, through their control of the technical design of the product or related services, what data are generated and how they can be accessed, even though they have no legal right to the data. It is therefore necessary to ensure that products are designed and manufactured and related services are provided in such a manner that data generated by their use are always easily accessible to the user».

[51] As mentioned before, Article 7 explicitly states that «The obligations of this Chapter shall not apply to data generated by the use of products manufactured or related services provided by enterprises that qualify as micro or small enterprises, as defined in Article 2 of the Annex to Recommendation 2003/361/EC, provided those enterprises do not have partner enterprises or linked enterprises as defined in Article 3 of the Annex to Recommendation 2003/361/EC which do not qualify as a micro or small enterprise».

same quality as is available to the data holder and, where applicable, continuously and in real-time». The User can now file a request to the Data Holder and force them to send their data to a Third Party, without having to incur in additional costs or wait a long time. Data Holder cannot use the data portability principle as an excuse to charge Users with transfer fees (which, for example, was often the case with telecommunication companies), nor they can speciously delay the transfer.

In addition, instead of making a request on their own name, Users, by law, can now give a power of attorney[52] to a third party, which acts in force of a contract of mandate. This provision is introduced for legal systems that do not have an existing discipline regarding mandate, and, in legal systems where this contract already exists, to force by law Data Holder to promptly comply with that mandate. In fact, even in legal systems in which special mandate is defined by a legal provision [53], it is not uncommon that large companies refuse to accept it in order to stonewall the User's request and avoid to comply with it. Thanks to this new provision, the possibility to use a mandate and the obligation to comply are clearly laid out by law.

Specularly to paragraph 6 of Article 4, paragraphs 6 and 7 coordinate the right to portability with that provided by GDPR, stressing the prevalence of the latter.

Paragraph 2 builds a bridge to the proposal for a Digital Markets Act of 2020, providing that "gatekeepers"[54] are not eligible to be considered "Third Parties" in this context. It also forbids them to:

- solicit or incentivize Users to make data, which has been obtained using the right of access, available to their services;
- solicit or incentivize Users to transfer data through to the right of portability;
- receive from Users the data obtained through the right of access.

This provision is intended to avoid giving gatekeepers (such as Google) even more

[52] By power of attorney we mean the unilateral act by which one person empowers another to represent him/her/them.

[53] E.g., the Civil Code, such as in Italy, Article 1703: «The mandate is the contract by which one party commits to perform one or more legal acts on behalf of the other».

[54] Gatekeepers are defined by the Digital Markets Act as providers of core platform services such as: «(a) online intermediation services; (b) online search engines; (c) online social networking services; (d) video-sharing platform services; (e) number-independent interpersonal communication services; (f) operating systems; (g) cloud computing services; (h) advertising services, including any advertising networks, advertising exchanges and any other advertising intermediation services, provided by a provider of any of the core platform services listed in points (a) to (g)»; provided that «(a) it has a significant impact on the internal market; (b) it operates a core platform service which serves as an important gateway for business users to reach end users; and (c) it enjoys an entrenched and durable position in its operations or it is foreseeable that it will enjoy such a position in the near future». In addition, it has to meet the following thresholds: «(a) the requirement in paragraph 1 point (a) where the undertaking to which it belongs achieves an annual EEA turnover equal to or above EUR 6.5 billion in the last three financial years, or where the average market capitalisation or the equivalent fair market value of the undertaking to which it belongs amounted to at least EUR 65 billion in the last financial year, and it provides a core platform service in at least three Member States; (b) the requirement in paragraph 1 point (b) where it provides a core platform service that has more than 45 million monthly active end users established or located in the Union and more than 10 000 yearly active business users established in the Union in the last financial year; for the purpose of the first subparagraph, monthly active end users shall refer to the average number of monthly active end users throughout the largest part of the last financial year; (c) the requirement in paragraph 1 point (c) where the thresholds in point (b) were met in each of the last three financial years».

business power than they already have, so that their economic position is not made stronger by a provision originally intended to help SMEs and consumers. The explicit exclusions also make sure that the User is not "tricked" into giving consent to the gatekeeper to re-use the data accessed according to the proposal. It is very common that Users do not read full texts of Terms and Conditions[55], therefore it is necessary to prevent exploitative practices that would allow them to easily gain access to an increased amount of User's data from third parties just by inserting a related clause in their Terms. Also, it prevents gatekeepers from obtaining data from Users through a compensation (monetary or not). This legal framework is complementing that of the Digital Markets Act to stem the bargaining and economic power of Big Techs by returning the control over data to consumers and by limiting their room for manoeuvre. If they wish to obtain the data, they cannot do this thanks to the Data Act.

Other provisions aimed at facilitating the right to portability require Data Holder to refrain from requesting «any information beyond what is necessary to verify the quality as user or as third party», and from keeping any information on the third party's requests beyond what is necessary to execute the request and «for the security and the maintenance of the data infrastructure».

In addition, exactly as provided for the right to access, a provision aimed at protecting trade secrets has been laid down: «the data holder shall not use any non-personal data generated by the use of the product or related service to derive insights about the economic situation, assets and production methods of or use by the third party that could undermine the commercial position of the third party on the markets in which the third party is active». However, a loophole also has been unwisely inserted: «Unless the third party has consented to such use and has the technical possibility to withdraw that consent at any time", enabling Data Holder to hide the consent form, as is often the case, under the general Terms and Conditions button. Is it any wonder why the Third Party would consent to let Data Holder derive information that potentially "could undermine the commercial position [...] on the markets».

Paragraph 8 protects the Data Holder specifying that trade secrets may only be disclosed to Third Parties insofar as they are strictly necessary to achieve the purpose agreed between the User and the Third Party (that is, in the context of the right to portability). The Third Party is required to adopt all necessary specific measures agreed upon to preserve the confidentiality of that information. The provision also requires that the Data Holder and the Third Party specify the nature of the data as trade secrets, and the security and organizational measures to preserve their confidentiality, in an agreement (which may well be inserted in the above-mentioned Terms and Conditions). This asymmetry of protection between Third Parties (which, according to this proposal, can only be non-gatekeepers) and Data Holders (which, at the contrary, generally are Big Techs) is out of tune with the purpose of the regulation.

On the other hand, interestingly, the provision forbid the Third Party to «deploy coercive means or abuse evident gaps in the technical infrastructure of the data holder designed to protect the data in order to obtain access to data», which in many coun-

[55] N. Steinfeld, *I agree to the terms and conditions:(How) do users read privacy policies online? An eye-tracking experiment*, in *Computers in human behavior*, 55, 2016, 992 ss.

tries would already *per se* constitute a criminal offense.

Article 6 imposes additional obligations to Third Parties, in order to protect Users from unfair use of the transferred data. First, similarly to GDPR, it introduces the principles of purpose and storage limitation, requiring Third Parties to limit the processing only to the purposes and under the conditions agreed with the User (also taking into account GDPR whenever personal data are involved), and it also requires them to delete the data as soon as they are no longer necessary to fulfil those purposes. In addition, according to the principle of fairness, it prohibits Third Parties to:

- coerce, deceive or manipulate the User in any way[56];
- use the received data to profile natural persons, unless it is necessary to provide the requested service;
- make the received data available to another third party, unless this is necessary to provide the requested service;
- make the received data available to gatekeepers;
- use, alone or through another party, the received data to develop a product that competes with the Data Holder's products;
- prevent the User to exercise the right to portability towards other parties.

The first paragraph of Article 8 forces Data Holders to abide to the principle of fairness, transparency, reasonableness, and non-discrimination[57], extending its scope not only to the sharing of data under this regulation, but also to any «other Union law or national legislation implementing Union law» that require them to share the data. Of course, fairness, reasonableness, and non-discrimination principles are fundamental principles of Union Law, therefore Data Holders are generally forced to apply them to natural persons. This provision, however, extends them, together with the transparency principle, to the general framework of data sharing, forcing Data Holders to comply with Chapters III and IV, and therefore to be subjected to the administrative fines provided by Article 33, even when they are making data available under a different piece of legislation. This is an interesting implication of the proposal, considering the upcoming set of legislation implementing the EU Digital Strategy.

To prevent situations of uncertainty and to attract the protection laid down by contractual law, paragraph 2 requires both Data Holders and Users to enter into a contract to regulate the terms of data availability (and are not obliged to provide more information than that strictly necessary to demonstrate compliance to the agreed contractual clauses[58]). It also states that clauses regarding the access to and use of the data or the liability and remedies for the breach or the termination of data-related obligations,

[56] The article specifies «by subverting or impairing the autonomy, decision-making or choices of the user, including by means of a digital interface with the user».

[57] «Where a data holder is obliged to make data available to a data recipient under Article 5 or under other Union law or national legislation implementing Union law, it shall do so under fair, reasonable and non-discriminatory terms and in a transparent manner in accordance with the provisions of this Chapter and Chapter IV».

[58] See para. 5: «Data holders and data recipients shall not be required to provide any information beyond what is necessary to verify compliance with the contractual terms agreed for making data available or their obligations under this Regulation or other applicable Union law or national legislation implementing Union law».

which are deemed to be unfair (according to Article 13) or in breach of User's rights under Chapter II, are nonbiding. It is unclear why the legislator has chosen the expression "non-binding" instead of "void", since it is referring to clauses that are contrary to mandatory provisions, which are non-derogable. In this context, it is reasonable to assume that the meaning is equal to "void", that is non-enforceable, non-remediable, and *ab origine* without any effect. Because of the aim of this provision, it is also presumed that the whole contract will be valid even without those void clauses.

With regards to the non-discrimination principle, it is forbidden to Data Holders to discriminate between "comparable categories"[59] of Data Recipients, including their partner enterprises or linked enterprises. In this context, the burden of proof is inverted: the Article provides that the Data Holder needs to demonstrate that no discrimination occurred. In addition to this provision, it is also forbidden to form a monopoly, making data available on an exclusive basis, unless explicitly requested by the User.

Article 9, following the principle of reasonableness, prescribes that any agreed compensation for making data available shall be reasonable, and in cases where the Data Recipient is a micro, small or medium enterprise, such compensation cannot exceed direct costs to comply with the request; however, the Article states that subsequent law may regulate its amount.

In the last paragraph, according to the principle of transparency, it is provided that Data Holders must provide in sufficient detail the criteria on which the calculation is based, in order to allow the Data Recipient to verify the reasonableness of the amount and where the direct costs originate.

The legislator provides for a dispute settlement mechanism to settle disputes in relation to the determination of fair, reasonable and non-discriminatory terms for and the transparent manner of making data available (Article 30), by establishing independent and certified bodies in each Member State.

6. Making data available in case of exceptional need

The right to access is not the only way in which the proposal requires Data Holders to share the data in their possession (as before, excluding small and micro enterprises). In fact, another important novelty of the Data Act is Article 14, which introduces the obligation to make data available to public bodies and authorities based on exceptional need circumstances, following a simple request. The concept of exceptional need is identified by Article 15 in

- the necessity to respond to a public emergency;
- the necessity to prevent a public emergency or to assist the recovery from a public emergency, when the data request is limited in time and scope;
- the necessity to fulfill a specific task in the public interest that has been explicitly provided by law, that is hindered by the lack of available data;

[59] The proposal does not draw any example or criteria to determine if a Data Recipient is deemed comparable. It could be presumed that reference should be made to size, sector, turnover.

- the impossibility for public sector body or Union institution, agency or body, to obtain such data by alternative means[60].

This provision may be seen as laying down a form of expropriation. The difference between the obligation to make data available towards Users and towards public bodies is that in the first case the data is generated by Users and consequently it can be argued that they are the legitimate owners, while in the latter case the obligation is towards a third party, who has no role in the generation of the data itself. In principle, third parties have no right over the data, and they are not part of the contract between Data Holders and Users. Only User can authorize Data Holders to share the data with Third Parties, conferring a power of attorney. In this case, not only the permission of the Users is bypassed, but they even have no possibility of challenging the request.
The value of data is now recognized worldwide and even became the core of many business models. For some companies, data is the only resource they have. In this context, it is clear that a sharing obligation means a transfer of assets from the company to the public authority, even if it is done for the public interest and in a situation of public emergency. Data can be considered as goods protected by international investment law,[61] but because of their nature, which allows to make copies, it is unlikely that the mandatory sharing obligation can be considered as direct expropriation. It is, however, possible to consider it as indirect expropriation.
On the other hand, it could be argued that the burden on companies is limited, as they are forced to share only a *copy* of their asset, thus continuing to exploit data for their own purposes. In addition, it has to be noted that the obligation only arises in limited cases, for example when it has not been possible to obtain the same data at market price. The company, in principle, could avoid the expropriation by preparing their data in advance to sell it to public authorities (when feasible and allowed by law).
According to article 17 of the EU Charter of Fundamental Rights[62], the rule of law must be respected when expropriating property in cases of public interest and a fair compensation must be paid.
However, Data Holders are not always compensated for the data sharing towards public entities, as in the case of public emergency they are required to make data available for free.
There are some guarantees for a fair and transparent request by public bodies. In fact, the request must abide some mandatory conditions. First, it must be specified what

[60] As some examples of unsuccessful attempts to obtain such data in other ways, the Article list the impossibility of purchasing the data on the market at market rates; the impossibility of obtaining the data by relying on existing obligations; and the fact that adopting new legislative measures would be too lengthy and could not ensure the timely availability of the data; it also mentions the circumstance that obtaining the data through the procedure laid down in the Data Act would substantively reduce the administrative burden for Data Holders or other enterprises.

[61] T. Peramatukorn, *Potential Expropriation Claims Against Data Sharing Requirements*, in *NYU Journal of International Law and Politics*, 54(1), 2021, 249 ss.

[62] «1. Everyone has the right to own, use, dispose of and bequeath his or her lawfully acquired possessions. No one may be deprived of his or her possessions, except in the public interest and in the cases and under the conditions provided for by law, subject to fair compensation being paid in good time for their loss. The use of property may be regulated by law in so far as is necessary for the general interest. 2. Intellectual property shall be protected».

data are required, the legal basis that allows the request, the deadline for complying to it or to challenge it. Article 18 provides that the Data Holder may decline or seek the modification of the request within 5 working days fin case of public emergency grounds and within 15 working days in other cases of exceptional need, if the data is unavailable, if the request does not meet the conditions laid down in Article 17 of the proposal, or if the requested data has already been provided in response to previously submitted request for the same purpose by another public body. In case of controversy, the case will be brought before the competent authority (Article 31).
Secondly, the public body cannot simply file a request, but it must demonstrate the exceptional need for which the data are requested, and it need to be proportionate to that exceptional need, in terms of the granularity and volume of the data requested and frequency of access of the data requested. The proposal requires that the legitimate aims of the Data Holder, the protection of trade secrets, and the cost and effort required to make the data available must be taken into account.
In addition, the purpose of the request, the intended use of the data requested, and the duration of that use must be specified.
Lastly, following the principle of data minimization, the request must concern non-personal data as much as possible. When personal data are needed, the Data Holder must take reasonable efforts to pseudonymise the data, if the request can be fulfilled with pseudonymised data. Regarding trade secrets, they can only be requested if the disclosure is strictly necessary to achieve the purpose of the request.
The public body must also inform the Data Holder of the penalties that will occur in the event of non-compliance with the request.
Additional guarantees are provided by Article 19, according to which the public body must respect the purpose limitation principle, implement technical and organisational measures that safeguard the rights and freedoms of data subjects whenever personal data are received, and follow the principle of storage limitation, destroying the data as soon as they are no longer necessary and informing the data holder that the data have been destroyed.

7. Transparency

Transparency is an overarching principle throughout the proposal, following the example of many legal instruments that are part of the EU Digital Strategy.
First, Article 3 introduces the right of information, stating that the subject that enter in a contract of purchase, rent, or lease with the User needs to provide the following information:

- the nature and volume of the data likely to be generated by the use of the product or related service;
- whether the data is likely to be generated continuously and in real-time;
- how the user may access those data;
- whether the manufacturer or the service provider intends to use the data itself or allow a third party to use the data and, if so, the purposes for which those data

will be used;
- whether the seller, renter or lessor is the data holder and, if not, the identity of the data holder (trading name and the geographical address);
- the means of communication to contact the data holder quickly and efficiently;
- how the user may request that the data are shared with a third-party;
- the user's right to lodge a complaint with the competent authority.

The right of information is designed in such a way that even companies providing their service for free through a software license are required to comply. Following the solution adopted by GDPR, Article 3 requires to disclose the data transfer to third parties, but also the purposes of the processing and the identity of the Data Holder.
Secondly, the transparency principle is translated in the obligation of the Data Holder to inform the Users on how the data may be accessed, before they enter into a contract (Recitals 20 and 23[63]). The right of access is itself a manifestation of the transparency principle.
In addition, the proposal prescribes transparency in contractual terms between Users and Data Holders with regards on how the latter intend to use the data generated by the use of their products, as explained in Recital 24[64].
Data Holders should also be transparent in explaining the justification of the compensation requested for making data available to third parties and the calculation criteria, in order to make it possible to assess the reasonableness of the request[65].
Public bodies are prescribed to be transparent as well when requesting data in cases of exceptional need, clearly stating the purpose of the request, the intended use of the data and the duration of that use[66]. They must notify the Data Holder when they

[63] Recital 23 explains the provisions regarding data access: «Before concluding a contract for the purchase, rent, or lease of a product or the provision of a related service, clear and sufficient information should be provided to the user on how the data generated may be accessed. This obligation provides transparency over the data generated and enhances the easy access for the user».

[64] «This Regulation [...] should not be understood as conferring any new right on the data holder to use data generated by the use of a product or related service. This applies in particular where the manufacturer is the data holder. In that case, the basis for the manufacturer to use non-personal data should be a contractual agreement between the manufacturer and the user. This agreement may be part of the sale, rent or lease agreement relating to the product. Any contractual term in the agreement stipulating that the data holder may use the data generated by the user of a product or related service should be transparent to the user, including as regards the purpose for which the data holder intends to use the data».

[65] As pointed out in Recital 47: «Transparency is an important principle to ensure that the compensation requested by the data holder is reasonable, or, in case the data recipient is a micro, small or medium-sized enterprise, that the compensation does not exceed the costs directly related to making the data available to the data recipient and is attributable to the individual request. In order to put the data recipient in the position to assess and verify that the compensation complies with the requirements under this Regulation, the data holder should provide to the data recipient the information for the calculation of the compensation with a sufficient degree of detail».

[66] Recital 61 explains that «[...] data requests by public sector bodies and by Union institution, agencies and bodies to data holders should be transparent and proportionate in terms of their scope of content and their granularity. The purpose of the request and the intended use of the data requested should be specific and clearly explained, while allowing appropriate flexibility for the requesting entity to perform its tasks in the public interest. The request should also respect the legitimate interests of the businesses to whom the request is made. [...] To ensure transparency, data requests made by public sector bodies and by Union institutions, agencies or bodies should be made public without undue delay by the entity

transmit or otherwise make data available to another public entity pursuant to Articles 17 and 21. They also need to inform the Data Holder about the penalties prescribed according to Article 33 for the infringement of the Data Act, as required by Article 17. However, in such cases no obligation of informing the Users is laid down by the current version of the proposal, unless the requested data set contains personal data, and this circumstance seems at odds with the general transparency obligation imposed in the rest of the act.

Lastly, DPSs are requested to enact the transparency principle when receiving a request to access the data from a foreign authority[67]. This provision ensures that Users in EU have the possibility to promptly prepare to defend their rights and seek legal assistance, since the foreign country requesting the data may have a very different legal system, with different limitation of action time frames that require an immediate reaction.

8. Regulating Smart Contracts

The proposal regulates also the use of Smart Contracts (SCs) for data sharing (Article 30). SCs «are pieces of code that enable users to write their own arbitrary rules for ownership, transaction formats and state transition functions. This means, two parties can digitally interact following a set of customized rules (defined by one of the parties) without the need of a third trusted party to secure the transaction. The deployment and/or interaction with smart contracts are immutable, permanent and irreversible. The process of deploying or interacting with an already deployed smart contract over the blockchain requires the users to connect to the peer-to-peer network through a client. Nodes in the network execute the smart contracts in return for a reward that keeps them incentivized. Rewards are referred to as gas, an execution fee willingly paid by nodes deploying or triggering the smart contracts»[68].

SCs are based on blockchain technology, which is «a distributed, decentralized, and tamper-proof shared ledger technology that allows peer-to-peer transmission»[69]. This technology has gained popularity in recent years as a method to mitigate privacy, security, and efficiency issues of centralized platforms[70], as in these systems a public

requesting the data and online public availability of all requests justified by a public emergency should be ensured».

[67] Recital 77 states in this regard that «Wherever possible under the terms of the data access request of the third country's authority, the provider of data processing services should be able to inform the customer whose data are being requested in order to verify the presence of a potential conflict of such access with Union or national rules, such as those on the protection of commercially sensitive data, including the protection of trade secrets and intellectual property rights and the contractual undertakings regarding confidentiality».

[68] E. Zaghloul – T. Li – J. Ren, *Security and privacy of electronic health records: Decentralized and hierarchical data sharing using smart contracts*, in *2019 International Conference on Computing, Networking and Communications (ICNC)*, IEEE, 2019, 375 ss.

[69] S. Xuan et al., *An incentive mechanism for data sharing based on blockchain with smart contracts*, in *Computers & Electrical Engineering*, 83, 2020, 106587.

[70] E. Zaghloul – T. Li – J. Ren, *Security and privacy of electronic health records*, cit.

ledger of records and transactions ownership is maintained by the network in real-time, secured by cryptography[71]. A key difference between centralized systems and blockchain-based systems is that the latter «do not suffer from a single point of failure and do not require a third trusted party to maintain the integrity of data ownership and flow»[72].

Because of the fact that once in the blockchain it is not possible to erase the data, which will be stored in a decentralized network, it must be ensured that no personal data is stored in the blockchain, in accordance with GDPR. This is one of the reasons that justify the need for regulating SCs.

The proposal requires whoever deploys SCs in the context of an agreement to make data available to comply with the following rules, being responsible for the compliance:

- robustness by design: ensure that the SC offers a very high degree of robustness by design, to avoid functional errors and to withstand manipulation by third parties;
- safe termination and interruption: ensure that it is possible to terminate the continued execution of transactions; the SC must be equipped with internal functions to stop or interrupt the operation to avoid future (accidental) executions;
- data archiving and continuity: foresee the possibility to archive transactional data, the SC logic and code, to keep the record of the operations performed on the data in the past (auditability), when a SC must be terminated or deactivated;
- access control: a SC must be protected through rigorous access control mechanisms and smart contract layers;
- conformity assessment: assess the compliance with the requirements and issue an EU declaration of conformity.

The provision also provides that a SC that meets the harmonised standards published in the Official Journal of the European Union is presumed to be in conformity with the above-mentioned requirements to the extent those standards cover them.

9. Provision regarding Data Processing Services

The Regulation introduces the concept of Data Processing Service, defined as «a digital service other than an online content service as defined in Article 2(5) of Regulation (EU) 2017/1128, provided to a customer, which enables on-demand administration and broad remote access to a scalable and elastic pool of shareable computing resources of a centralised, distributed or highly distributed nature». The reference is obviously to cloud services providers, such as Microsoft, Amazon, Google. The proposal anticipates the expansion in the market related to DPSs, which will be likely prompted by the enacting of the Data Act itself, since, by limiting the power of large foreign companies, it will enhance the competition for European actors.

A cloud computing service is a common IT solution that allows Users to store and

[71] *Ibid.*

[72] *Ibid.*

process their data on third-party IT facilities, such as servers, computing power, and software, accessible on demand through Internet technologies[73].[74]There are many different types of cloud services and the simplest is the mere storage solution (such as Dropbox), which allows Users to just upload and store their data online. Because Users are physically giving a copy of their data (uploading it online) to a third party, it basically can be thought of as an agreement of mixed nature, composed of a custodial contract and a service contract, in which one party (the DPS provider) commits to keep and guard the other party's data, making them available at request, and sometimes also to provide other services (such as software applications that provide analysis tools) through their own means and facilities, and the depositor commits to pay a fee for the whole service. Part of legal scholars consider it as a mixed contract composed of a lease agreement and a service agreement,[75] others as a mere service contract, and others as a custodial contract[76] when no other service but the storage space is provided. The ownership of the data remains of the depositor, while the cloud service provider is a mere possessor and custodian, and generally has no intention of exercising property rights on the data (*animus detinendi*), unless otherwise agreed.
The qualification of the contract is very important to understand duties and rights of the parties. For example, in the custodial contract, the custodian has the duty to i) make the objects available to the depositor at request, in the same state they were handed; ii) keep the objects safe in their facilities and prevent them from being stolen or accessed, or used by third parties, with the same *diligentiam quam in rebus suis adhibere solet*;[77] iii) not making use of the objects for their own purposes (*Depositum consistit ex custodia non ex usu*) iv) return the objects and their unearned income to the depositor at the end of the contract, in the same state they were handed. In the lease contract, at the contrary, the lessor has the duty to i) make their facilities available to the lessee in a good state ii) keep the facilities available and accessible during the whole duration of the contract so that the lessee can use it as agreed iii) repair and perform the maintenance of the facilities iii) prevent other parties from interrupting of disturbing the use of the facilities. On the other hand, in the service contract, the contractor has the duty of i) render the agreed services through their own means and facilities and at their own risk ii) keep the objects safe and prevent them from being stolen, accessed or used by third parties, with the same *diligentiam quam in rebus suis adhibere solet* iii) let the commissioner check the status and performance of the services iv) guarantee that the services are executed as agreed and without flaws v i) make the objects available to the commissioner at request.

[73] The National Institute of Standards and Technology (NIST) defines it as «a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction».

[74] M. Hogan et al., *Nist cloud computing standards roadmap*, in *NIST Special Publication*, 35, 2011, 6 ss.

[75] A. Mantelero, *Il contratto per l'erogazione alle imprese di servizi di cloud computing (Cloud Computing Contracts: B2B)*, in *Contratto e impresa*, 4-5, 2012, 1216 ss.

[76] G. Sicchiero, *Il contratto di deposito di beni immateriali: i-cloud e files upload*, in *Contratto e Impresa*, 2, 2018, 681 ss.

[77] *Ibid.*

Cloud computing contracts are usually composed of three distinguished documents, one containing the general conditions of the service, one inherent the polices regarding the behaviour of the parties, and one prescribing the modalities of the data processing.[78] However, because of the unbalance of powers between the cloud providers and their clients, these terms are often unilaterally drafted and imposed, and no negotiation of the clauses is possible. To tackle this issue, the proposal provided some mandatory terms, to be included in all contracts, protecting Users from vexatious contractual clauses. At Articles 23, 24, 25, and 26, some guidelines are drawn to eliminate obstacles to the switching between providers of DPS, in order to ensure interoperability, both from a technical and business perspective. This is motivated by the necessity of preventing "lock-in" practices, which are very common in cloud computing contracts.

In particular, the provisions are aimed at removing commercial, technical, contractual and organisational obstacles to let Users switch between different DPSs. Such obstacles are first identified in contractual practices preventing Users from:

- cancelling the contract with more than 30 days of notice;
- entering into a contract with a different DPSs which provide the same service type;
- transferring their data, applications and other digital assets to other DPSs;
- maintaining functional equivalence of the service in the IT-environment of the DPSs to which they are switching.

To protect the User from the most common unfair contractual terms, Article 24 forces DPSs to clearly set in a contract their obligations and the rights of the customer related to the switching between providers[79]. It prescribes that at least the following elements must be included in the contract:

- the possibility for customers to switch to a DPS offered by a different company, or to port all data, applications and digital assets generated by them to an on-premise system. The request must be fulfilled within 30 calendar days, during which the DPS must assist and, if technically feasible, complete the switching process, and ensure full continuity in the functions or services;
- an exhaustive specification of all data and application categories exportable during the switching process, including, at minimum, all data imported by the customer at the inception of the service agreement and all data and metadata created by the customer and by the use of the service during the period the service was provided, including configuration parameters, security settings, access rights and access logs to the service;
- a minimum period for data retrieval of at least 30 calendar days, starting after the termination of the transition period that was agreed between the customer and the service provider.

[78] A. Mantelero, *Il contratto per l'erogazione alle imprese di servizi di cloud computing,* cit.; S. Bradshaw – C. Millard – I. Walden, *Contracts for clouds: Comparison and analysis of the terms and conditions of cloud computing services*, in *International Journal of Law and Information Technology*, 19(3), 2011, 187 ss.

[79] The provision stresses the fact that it is without prejudice to Directive (EU) 2019/770 of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services.

It is also provided that, if the mandatory transition period of 30 days is technically unfeasible, the DPS must notify the customer within 7 days, duly motivating the technical unfeasibility with a detailed report and indicating an alternative transition period of maximum 6 months, during which full service continuity must be ensured.

9.1 Interoperability

The proposal also establishes a right to data interoperability for the User, in order to remove technical obstacles for the switching. Interoperability means that different cloud solutions are able to communicate and exchange data between each other's. In concrete terms, it allows users to transfer their data from one provider to another across heterogeneous hardware and software resources, without losing any data, in terms of functionality or accessibility.

In fact, in order to be able to switch from one DPS provider to another, Users need to be able to i) access their data before their contract is ending, or soon after (accessibility); ii) transfer their data to the other provider, e.g., by downloading it and then uploading to the new servers, or by directly transferring it (portability); iii) have their data in a format that is compatible with the new provider's systems (interoperability). In commercial practice, it often happens that vendors adopt proprietary format that prevents Users to efficiently port their data in different environments (the so-called lock-in practice). If the format is not compatible with the new provider's system, and it is not possible to convert it to a compatible format, then the User loses its data. This often happens for applications specifically built for a certain environment (e.g., Microsoft Azure).

Although many studies highlight the fact that lock-in practices constitute a major barrier to cloud computing adoption,[80] the research on cloud interoperability issues is limited.[81] Some industry bodies have tried to develop standards, but the issues has not been solved so far. The Data Act aims at tackling the issue at least with regards to portability of Users' data.

Firstly, in case the cloud services «concern scalable and elastic computing resources limited to infrastructural elements such as servers, networks and the virtual resources necessary for operating the infrastructure», but «do not provide access to the operating services, software and applications that are stored, otherwise processed, or deployed on those infrastructural elements», that is the most basic DPS service, the DPS must ensure that the customer, after switching to a different provider offering the same kind of services, is able to enjoy «functional equivalence in the use of the new service». The reference is probably to cloud computing providing storage services, however the wording is not very clear and may lead to uncertainty regarding the

[80] D. Petcu – A. V. Vasilakos, *Portability in clouds: approaches and research opportunities*, in *Scalable Computing: Practice and Experience*, 15(3), 2014, 251 ss.; J. Opara-Martins – R. Sahandi – F. Tian, *Critical analysis of vendor lock-in and its impact on cloud computing migration: a business perspective*, in *Journal of Cloud Computing*, 5(1), 2016, 1 ss.

[81] X. V. Wang – L. Wang – R. Gördes. *Interoperability in cloud manufacturing: a case study on private cloud structure for SMEs*, in *International Journal of Computer Integrated Manufacturing*, 31(7), 2018, 653 ss.

subjects of this provision.
Secondly, for all other services, which means those providing access to «the operating services, software and applications that are stored, otherwise processed, or deployed on those infrastructural elements», the proposal prescribes that DPSs must «make open interfaces publicly available and free of charge and ensure compatibility with open interoperability specifications or European standards for interoperability», where existing. If the standards do not exist, the DPS must, at the request of the customer, export all generated or co-generated data «in a structured, commonly used and machine-readable format». The wording is again unclear and the impact of this provision is still uncertain. Is the legislator expecting Amazon to create an «open interfaces publicly available and free of charge» for their services, or just for the switching of data to a different service, in order to provide functional equivalence?
The Recitals stress the necessity of an intervention at EU level, however it is unclear how DPSs will need to comply to the Data Act in the meantime that those standards are developed and tested. It is hoped that these provisions will be modified by the EU bodies before the regulation is enacted.

9.2 International transfer of data

Similarly to GDPR, the legislator provided for some limit to the transfer of data outside the EU, requiring DPSs to «take all reasonable technical, legal and organisational measures, including contractual arrangements, in order to prevent international transfer or governmental access to non-personal data held in the Union where such transfer or access would create a conflict with Union law or the national law of the relevant Member State». Even if it is only related to nonpersonal data, the provision was clearly inspired by the Schrems II judgments of the Court of Justice of the European Union (CJEU) in 2020, which invalidated the Privacy Shield between the US and the EU. In fact, the judgment highlighted that the US law is very invasive of privacy even when data are not located in the US, because companies are forced to transfer the data in their possession to the US authorities.
The European Data Protection Board noted that «the US CLOUD Act also extends the possibility to request data wherever they are stored or located to the whole of Chapter 121 of USC Title 18 on 'Stored wired and electronic communications and transactional records access'. To our understanding, this means that this applies to many other data collection avenues, in particular to requests to access content data through a court order or a subpoena (either administrative, grand jury or trial subpoena). It also applies to requests for non-content data (so-called 'metadata') under §2703 of Chapter 121 USC Title 1811, which covers (subsection (c)) a whole range of avenues, including warrants and court orders, but also avenues that do not necessarily require judge intervention or a probable cause test, such as formal written requests or subpoenas. Furthermore, the US CLOUD Act opens the possibility for service providers to 'intercept or disclose the contents of a wire or electronic communication in response to an order from a foreign government' (this covers real-time interception)

under the condition that this foreign government has entered into an executive agreement with the US». This circumstance poses a risk not only for personal data, but also for trade secrets, government classified documents, and other data that may be relevant for the protection of EU interests.

The Data Act aims at making sure that foreign data centers, on which usually cloud providers rely, do not put EU data at risk by communicating relevant information to foreign governments, not only in the US, but also in other countries where the relationships are tenser. Therefore, it is provided that even when a judicial or administrative decision requiring the transfer of data is present, it «may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or any such agreement between the requesting third country and a Member State».

In the absence of such an international agreement, the transfer to or access to the data by third-country authorities can take place only in three cases, notably when the rule of law is respected:

- where the third-country system requires that the reasons and proportionality of the decision are set out, and it requires such decision to be specific, for instance by establishing a sufficient link to certain suspected persons, or infringements;
- the DPS can file a reasoned objection, which is subject to a review by a competent court in the third-country;
- the competent court or authority is empowered, under the law of that country, to take duly into account the relevant legal interests of the provider of the data protected by Union law or national law of the relevant Member
- State.

The DPS which receives the request according to a judicial or administrative decision has the possibility to ask the opinion of the relevant competent authorities of the EU to be sure that the required conditions are met, especially if commercially sensitive data, or national security or defense interests of the Union or its Member States are at stake.

While it may be easy to make sure that European DPSs respect this provision, it might be questionable to assume that foreign companies would refuse to comply with a decision of their own country, therefore the impact of this provision might be limited. It would be wise for the legislator to provide a different compliance mechanism other than just providing a body that will give an advice on the transfer. For example, a provision may be inserted to give companies a stronger leverage to oppose their government, such as a judicial decision from a European Court. In the case of GDPR, the enforcement mechanism is just limited to the stopping of all transfer to third countries. It is unknown, however, if this solution will be adopted in the case of the Data Act, and how it will be enforced in practice.

10. Provisions regarding unilaterally imposed unfair clauses

The new legal framework tackles the issue of unfair contractual terms unilaterally imposed on a micro enterprises and SMEs by providing, in Chapter IV of the proposal, some mandatory terms, non-derogable in any way by the parties. The discipline is borrowed by consumer protection law, and in particular Directive 93/13/EEC.
The introduction of this discipline for the protection of non-consumers builds upon a long tradition both at EU level and at national level; the theme of unfair commercial practices in B2B contracts has seen multiple failed attempt of regulation within the EU[82], while it has successfully been implemented in some Member States[83]. Recently, a further step towards the harmonization of the discipline has been made by the Regulation on promoting fairness and transparency for business users of online intermediation services, which provides some rules to prevent unfair contractual practices.
The scope of application of the Chapter is not restricted to specific cases, but it applies to all contracts regardless of their nature, field, or duration, provided that they pertain to the access to and use of data, liability, remedies for the breach, or termination of data related obligations. In fact, it provides that, when it comes to those specific subject, unilaterally imposed terms are not binding on micro enterprises and SMEs if they are unfair. The concept of unfairness was introduced by Directive 93/13/EEC, which provides that contractual terms which have not been individually negotiated must be considered unfair whenever they cause an imbalance of rights and obligations against the weaker party[84].
"Unilaterally imposed" means that «it has been supplied by one contracting party and the other contracting party has not been able to influence its content despite an attempt to negotiate it». The concept is slightly different from that of consumer protection enshrined in Directive 93/13/EEC[85], as it does not refer only to pre-formulated standard contracts, but, being in the context of B2B relationships, it expands its scope to clauses that have been individually negotiated outside the context of a pre-formulated standard contract, albeit without success. Companies have more contracting power than consumer, therefore they might be able to negotiate many clauses in a contract; however, larger enterprises are still able to impose most of their own terms to the detriment of their counterpart.

[82] Such as the proposal for a Common European Sales Law in 2011, which can now be considered shipwrecked.

[83] See, for example, in Belgium, the Law of 4 April 2019, and, in Italy, Articles 1341 and 1342 of the Civil Code.

[84] As drawn up by Article 3: «A contractual term which has not been individually negotiated shall be regarded as unfair if, contrary to the requirement of good faith, it causes a significant imbalance in the parties' rights and obligations arising under the contract, to the detriment of the consumer».

[85] Article 3: «A term shall always be regarded as not individually negotiated where it has been drafted in advance and the consumer has therefore not been able to influence the substance of the term, particularly in the context of a pre-formulated standard contract. The fact that certain aspects of a term or one specific term have been individually negotiated shall not exclude the application of this Article to the rest of a contract if an overall assessment of the contract indicates that it is nevertheless a pre-formulated standard contract».

Like in the above-mentioned Directive[86], the burden of proof is reversed on the contracting party that supplied a contractual term, that is, the other party can claim that the term was unilaterally imposed without having to prove the claim. This provision is intended to protect the weaker part from the most common unfair practices of larger companies, which usually have the bargaining power to decide the most favourable terms for themselves.

The Directive makes reference to the criterion of objective good faith, which is transposed in the text of the novel legislation. The second paragraph of Article 13, in fact, defines unfairness as the grossly deviation from good commercial practice in data access and use, contrary to good faith and fair dealing. Good faith and fair dealing are then the measure that makes it possible to distinguish between lawful practices and illicit ones. The third paragraph draws a list of clauses that are considered unfair by law:

excluding or limiting the liability of the party that unilaterally imposed the term for intentional acts or gross negligence;

excluding the remedies available to the party upon whom the term has been unilaterally imposed in case of non-performance of contractual obligations, or the liability of the party that unilaterally imposed the term, in case of breach of those obligations;

giving the party that unilaterally imposed the term the exclusive right to determine whether the data supplied are in conformity with the contract or to interpret any term of the contract.

Other terms are presumed unfair if their object or effect is to:

- «inappropriately limit the remedies in case of non-performance of contractual obligations or the liability in case of breach of those obligations;
- allow the party that unilaterally imposed the term to access and use data of the other contracting party in a manner that is significantly detrimental to the legitimate interests of the other contracting party;
- prevent the party upon whom the term has been unilaterally imposed from using the data contributed or generated by that party during the period of the contract, or to limit the use of such data to the extent that that party is not entitled to use, capture, access or control such data or exploit the value of such data in a proportionate manner;
- prevent the party upon whom the term has been unilaterally imposed from obtaining a copy of the data contributed or generated by that party during the period of the contract or within a reasonable period after the termination thereof;
- enable the party that unilaterally imposed the term to terminate the contract with an unreasonably short notice, taking into consideration the reasonable possibilities of the other contracting party to switch to an alternative and comparable service and the financial detriment caused by such termination, except where there are serious grounds for doing so».

The proposal follows the principle *utile per inutile non vitiatur*, therefore providing that if a clause is non-binding, it doesn't invalidate the whole contract.

As it is easy to note, the list is significantly shorter than the one provided by the An-

[86] Article 3: «Where any seller or supplier claims that a standard term has been individually negotiated, the burden of proof in this respect shall be incumbent on him».

nex to Directive 93/13/EEC, although it can be argued that the regulation does not intend to establish a *numerus clausus* of terms, but different cases are left open by the general provision contained in the second paragraph of Article 13.
The list does not mention the most common clauses that are present in IoT and cloud computing contracts, such as the ones granting to the Data Holder the indiscriminate right to make use of the data as they wish (e.g., to improve their services, to sell the data to third parties, to profile users for advertisement purposes), as they fall out of scope of the proposal. However, in a study conducted by EY in 2018 about unfair cloud computing contracts, most SMEs reported a number of problems, such as unilateral changes of the contract, that lead to significant economic detriment, which have not yet been addressed by the legislator.[87]
This circumstance limits the significance of the regulation and it is a missed chance to complement the provisions of GDPR. Gaining access to the data is a good starting point for Users, but it does not significantly affect the EU market. Larger companies do not have an advantage only because of the mere fact that they are the only ones being able to access Users' data, but mostly because they have larger and better means to exploit that data without any control, including selling it to advertisers. While GDPR was able to limit these practices, even if not significantly, the Data Act fails to have the same impact.

11. Conclusion

The new proposal complements the legislative framework of the European Digital Strategy and confers to Users new rights, complementing those envisaged by GDPR. It is, in fact, shaped with a view of GDPR, of which it mimics the rights of access, right to portability, and the principles of transparency, purpose limitation, storage limitation, the limitations to international transfers, and the enforcement model. It also takes into account the principles of fairness, reasonableness and non-discrimination, extending them to the whole data sharing legal framework. Users are now empowered to obtain, port, and use the data they generate through IoT devices.
It is aimed at balancing the market and protecting consumers and smaller enterprises against the power of larger companies dominating the IoT field. To avoid claims of copyright infringement related to the IoT data, which could hinder the right of access, it modifies the Database Directive, excluding the application of the *sui generis* right. It also provides for a novel discipline of unfair clauses, previously limited to business-to-consumer relationships.
In addition, the right of access is extended to public sector bodies, as they are now able to directly request IoT data in case of exceptional need, and Data Holders have only limited grounds for refusing to disclose those data.
The proposal regulates cloud computing and smart contracts as well, providing for the first time some interoperability requirements.

[87] European Commission, *Study on the Economic Detriment to Small and Medium-Sized Enterprises Arising from Unfair and Unbalanced Cloud Computing Contracts*, 2018.

However, some issues still remain open, such as the fact that European standards for interoperability are still needed in order to obtain an effective enacting of the new provisions on cloud computing; the fact that there seems to be an imbalance between the provisions regarding Data Holders' trade secrets protection and those regarding Third Parties; the limited number of clauses deemed as unfair.
Lastly, the proposal does not go as far as fully regulating the way in which Data Holder can use Users' data, therefore failing to limit the true power of larger enterprises.
It is hoped that the upcoming revisions of the proposal will take all of these aspects into consideration.