INSTITUTE OF PUBLIC POLICY

LISBON

POLICY PAPER 26

European Data Strategy: Regulatory & Policy Aspects

Steffen Hoernig (Nova SBE, IPP)

André Ilharco (IPP)

Policy Papers

Policy Papers by Institute of Public Policy aim to support the public debate with concise contributions, featuring an accurate analysis of public policy, from which clear recommendations are derived.

The authors

Steffen Hoernig is Professor of Economics at Nova SBE, Lisbon, and a board member of IPP. André Ilharco is a researcher at IPP.

About Institute of Public Policy

The Institute of Public Policy is a Portuguese, academic and independent think tank. Its mission is to contribute to the continuous improvement of the analysis and public debate of institutions and public policies, with emphasis on Portugal and Europe, through the creation and dissemination of relevant research.

Table of contents

1. Overview and purpose of the European Data Strategy 3
2. Legal Instruments 5
2.1. Data Governance Act: Institutional Framework for data sharing. Intended to create trust that rights and freedoms are respected when data are shared. 5
2.2. Data Act: Creating a fair data economy – Sharing of IoT data 6
2.3. The nine European common data spaces 7
2.4. Open Data Directive: access to data held by public institutions 9
3. Interactions with other EU legal Instruments 11
3.1. Open Declaration of Digital Rights of 2022 11
3.2. Digital Markets Act and Digital Services Act 11
3.3. GDPR of 2016, ePrivacy directive of 2002 and ePrivacy Regulation 12
3.4. Proposals for AI Act of April 2021 and AI Liability Directive 13
3.5. Proposal for Gigabit Infrastructure Act of February 2023 13
3.6. Intellectual property rights 14
4. Effects of the European Data Strategy in Three Dimensions 15
4.1. The Political Dimension 15
4.2. The Economic Dimension 16
4.3. The Regulatory Dimension 18
5. Impact on stakeholders 21
5.1. Citizens/individuals/users 21
5.2. Businesses and SMEs 23
5.3. Civil society and Data Altruism 26
5.4. Producers of IoT devices 27
5.5. Providers of cloud services 27
5.6. National Regulatory Authorities 28
5.7. Research institutions 28
5.8. Public Administration 29
5.9. Countries 31
References 33

1. Overview and purpose of the European Data Strategy[1]

The EU Data Strategy is based on the Communication issued by the European Commission in 2020[2]. It is a 5-year plan and strategy that presents a vision of a data-driven economy in the EU and sets the guidelines for the future regulatory framework. It will ensure that data can flow within the EU and across sectors, maximizing its potential for innovation. Secondly, this framework will mirror European rules and values in its application to fields such as personal and non-personal data protection, consumer protection legislation or competition law. The strategy adopted by the EU differs from other data markets such as the US and China. Its vision is based on a human-centred economy and society. Thirdly, it will address the rules for access to and use of data - these must be "fair, practical and clear", and transparent and trustworthy data governance mechanisms will be designed. The approach to international data flows shall be open, but assertive, and always based on European values such as fair competition or protection of individuals' rights.

The Data Governance Act (DGA) and the recently proposed Data Act (DA) constitute two significant steps in the implementation of the EU Data Strategy. The DGA instructs Member States and their designated "competent authorities" to maximize their openness regarding the sharing of data held by public entities, even in the case of confidential data. The DGA also outlines the role of and rules for data intermediaries (further on explained) and incentivizes data altruism organizations and practices. On the other hand, the DA is concerned with fairness and autonomy in data markets, especially for the Internet of Things (IoT). It defends users' rights to their data and their (re)use, while it also determines that fair and reasonable access conditions must be provided by data holders on a number of occasions in the presence of market power. While the DGA is focused on the institutional framework for data sharing, namely through the indication of clear responsibilities for the main actors in the data economy, the DA will regulate who can use and access what data and for which purposes in the EU.

Additionally, the 2020 Data Strategy proposes the creation of Common European Data Spaces focused on the sharing and pooling of data across the EU and sectors. These data spaces are expected to cover the nine areas described below. Here, the Commission establishes that data must be made

[1] This IPP Policy paper contains an extended version of the IPP chapter in the PromethEUs network paper "EU Data Strategy. A multifaceted perspective from Southern European countries", June 2023.
[2] COM/2020/66, "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". https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1593073685620&uri=CELEX%3A52020D C0066

available according to the FAIR principle (Findable, Accessible, Interoperable and Re-usable), which follows the spirit both of the DGA and the DA.

With the creation of nine European data spaces, these Acts point to the European vision of a data market, based on European principles such as fair competition or an open and non-discriminatory market: A data economy where “undertakings compete on quality of services, and not on the amount of data they control” (EU Data Strategy, May 2022, Recital 2).

2. Legal Instruments

2.1. Data Governance Act: Institutional Framework for data sharing. Intended to create trust that rights and freedoms are respected when data are shared.

The DGA came into force on 23 June 2022 and will come into effect on 24 September 2023. It creates a regulatory framework that seeks to promote trust in the European data environment and markets.

First, the DGA sets out a framework for the re-use of publicly held protected data, without creating any right of access. For example, sensitive data such as those related to national or public security are explicitly excluded. The Open Data Directive of 2019 already mandates the release of public sector data, however, several types of data protected as confidential, intellectual property rights, or personal data not otherwise protected by the GDPR, were not covered by this Directive, which left a significant gap in the "data map" envisaged by the EU Data Strategy. The DGA prohibits the Member States' public bodies to enter into exclusive data-sharing agreements or concede these rights exclusively to any entity. The only allowed exception is if "an exclusive right to re-use data (…) [is] necessary for the provision of a service (…) in the general interest that would not otherwise be possible". Competent authorities, nominated under the DGA and in charge of supervising the implementation, are entitled to impose other conditions on the terms of re-use, making sure they are non-discriminatory, proportionate, objectively justified and that they do not restrict competition.

Second, the DGA defines data intermediation services providers (DISPs) as providing "a service which aims to establish commercial relationships for the purposes of data sharing between an undetermined number of data subjects and data holders on the one hand and data users on the other …". According to the Commission, these entities will be essential to assure fair competition and the availability of data across countries and sectors, especially for start-ups and SMEs. The Commission proposes a control mechanism for DISPs, based on mandatory registration with (although no regulatory approval is required) and ex-post supervision by the competent authorities, including sanctions for misdemeanours, for these entities.

Third, the Data Governance Act presents the concept of "data altruism organizations" (DAOs). Data altruism is defined as the "voluntary sharing of data on the basis of the consent of data subjects to process personal data pertaining to them, or permissions of data holders to allow the use of their non-personal data without seeking or receiving a reward that goes beyond compensation related to the costs" of sharing their data for objectives of general interest. This definition covers purposes such as healthcare, mobility, provision of public services, official statistics, among others. The Commission will

publish a “rulebook” setting out further instructions and information requirements for recognition as DAO and a European Altruism Consent Form for data subjects.

Fourth, the DGA proposes the establishment of national “competent authorities” and the creation of a European Data Innovation Board (EDIB), a technical body composed of experts representing competent authorities along with other European institutions and expert bodies. The main tasks of the EDIB will be to advise and assist the Commission, as well as to propose guidelines for the common European data spaces.

Finally, the DGA defines some rules about lawful and unlawful transfers of data to third countries. Any entity receiving data under this Regulation must take all reasonable measures, including contractual arrangements, to prevent the international transfer or governmental access to non-personal data held in the Union where such action would create a conflict with Union or each Member States’ national laws. Third countries’ court or administrative decisions to transfer or give access to non-personal data held in the Union shall be recognised only if based on an international agreement in force between the requesting third country and the Union or the Member State.

2.2. Data Act: Creating a fair data economy – Sharing of IoT data

In February 2022, the Commission published its proposal for the DA, regulating who can use and access what data for which purposes across all the economic sectors of the EU. By data, the Commission means “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”. The type of data targeted by the DA is the data generated by connected devices, be it personal or non-personal data. This means it targets principally products and services connected to the internet of things (IoT).

Directly affected by the new rights and obligations envisioned in the DA are stakeholders such as the producers and manufacturers of the connected products and related services, its users, data holders (legal or natural person who has the right/obligation to make certain data available), cloud services providers in the EU, data processing services providers or public bodies that require data holders to provide a specific data in exceptional circumstances. The DA states responsibilities, duties, rights and obligations for these stakeholders in specific topics such as data access and sharing or the protection of trade secrets and confidential information.

Regarding data access and sharing, connected products and related services must be made in a way to allow users to access their data easily, and to be informed pre-purchase about the nature and the volume of data likely to be generated by its use. Data holders will be obliged to make the data available to third parties upon user request. Also, trade secrets must be protected when data are shared.

Data holders are entitled to reasonable compensation for making data available to third parties. However, there are exceptions such as the provision of data to public bodies in exceptional circumstances, such as public emergencies, where data must be granted without delay and free of charge.

Finally, the DA seeks to facilitate the switching of business customers between cloud and data processing services[3] and to adapt contract law to "prevent the exploitation of contractual imbalances that hinder fair data access and use for micro, small or medium-sized enterprises." The latter is part of a set of rules to minimize the regulatory burden on SMEs and protect them from potential abuses by larger market players. Also connected to the protection of SMEs against larger players, the DA typifies situations when contractual terms regarding the access or use of larger companies' data by SMEs are to be considered unfair. Excluding the price to be paid, both contracting parties must be able to influence the negotiations of the terms of the contract.

Since the publication of the initial proposal of the DA by the Commission, both the European Parliament and the European Council have proposed several amendments to this text. On March 14th, 2023, the European Parliament (EP) published its amended version of the DA for the trilogue.[4] In this augmented version, the EP tries to clarify the DA text by providing more details about which kind of data and stakeholders are targeted by each disposition, renames the national competent authorities as "data coordinators", and reinforces provisions on trade secrets protection, among other revisions. The March 17th version of the Council[5] has common concerns with the EP text, namely the need to clarify concepts and dispositions and the strengthening of trade secrets protection. This version also includes modifications on the dispositions regarding the interplay between the DA and sectoral and horizontal legislation, such as the GDPR. It also provides clarification on the terms of "reasonable compensation", includes SMEs (under certain circumstances) in the obligation to share their data with public authorities in situations of exceptional need, and includes modifications concerning the freedom of consumers in switching data processing services.[6]

2.3. The nine European common data spaces

To reinforce the creation of a data economy in the EU, the Commission proposed the establishment of thematic data spaces. These nine data spaces are created to nurture an informational ecosystem

[3] The proposal for a digital bill unveiled by the French government on May 10th, 2023, includes rules very similar to those in the DA for the switching of cloud providers, with the aim to speed up significantly the protection of both French cloud providers and cloud users (Euractiv 2023, France 2023), as compared to the DA approval timeline.
[4] See https://www.europarl.europa.eu/doceo/document/TA-9-2023-0069_EN.html.
[5] European Council 2022/0047(COD) of 17 March 2023. Available at https://data.consilium.europa.eu/doc/document/ST-7413-2023-INIT/en/pdf.
[6] The trilogue negotiations finished with an agreement at the end of June 2023, but the final text will not be consolidated and publicly available for another few months.

based on the free flow of non-personal data across borders and sectors and between businesses, academia, relevant stakeholders, and the public sector. Such data spaces would be:

- **An Industrial (Manufacturing) Data Space:** According to the EU Data Strategy, the potential value of the use of non-personal data in manufacturing at € 1.5 trillion by 2027. This data space will be designed to significantly enhance the competitiveness of European industries. Together with Regulation 2018/1807, the DA is set to determine new dispositions regarding the usage rights of co-generated industrial data (IoT data created in industrial settings).

- **A Green Deal Data Space:** This data space will make available data concerning climate change, circular economy, zero-pollution, biodiversity, deforestation, and compliance assurance. For this, the Commission mentions the revision of older legislation and the "GreenData4All" initiative. Also, in line with the Data Act, the Green Deal Data Space will start collecting, sharing, processing, and analysing data of reusable data services on a large scale to assist in assuring compliance with environmental legislation.

- **A Mobility Data Space:** This data space will be focused on the processing and availability of the large amounts of data expected to be generated by automobiles (electric or not) on their movement, maintenance, and reparation. The predicted growth of transport activities in the next decades makes this data space fundamental for topics such as the environment or smart cities. New interconnected platforms will be available to provide data on issues such as road safety, traffic and multi-modal travel information services, generated both by the public and the private sectors.

- **A Health Data Space:** The Health Data Space aims to increase the quality of healthcare while decreasing its costs and fostering innovation. The implementation of EU citizens' rights to re-use and port their personal health data is fragmented within and between the Member States. Health institutions' rules of governance also differ strongly, especially between countries. According to the Commission, the Health Data Space will require the deployment of new legislative and non-legislative measures, data infrastructures and capacities focused on the interoperability and flow of health data across institutions and borders.

- **A Financial Data Space:** EU regulation and the 2015 Payment Services Directive fostered the openness of the financial markets and institutions. The Commission seeks to promote integrated capital markets, improve market transparency, and support sustainable finance in the EU. For this, the Commission promises to explore future additional steps not mentioned in the Data Strategy and to further facilitate access to public disclosures of financial data or supervisory reporting through this data space.

- **An Energy Data Space:** The objective of the Energy Data Space is to facilitate innovative solutions and support the decarbonization of the energy system. For this, the Commission is

determined to legally require interoperability and transparent procedures for access to data, as well as to promote interoperability in smart buildings and products, their energy efficiency, improved consumption, and integration of renewable energies.

- **An Agriculture Data Space:** The Commission seeks to go further than the current code of conduct on contractual agreements and common practices in agriculture regarding the sharing and pooling of data. It aims to fulfil the potential impact of data in agriculture through interconnecting the processing of agricultural, machinery, earth observation, meteorological and other types of data. The accessibility of such data in a common data space should promote fair contractual relations and strengthen the capacities for monitoring and implementing common policies while reducing the administrative burden for EU Member States' public authorities.

- **Public Administration Data Spaces:** Data quality in public procurement and its accessibility differ across EU Member States. The public administration data spaces will focus on law and public procurement data, as these are understood to be fundamental to promote transparency and accountability of public spending, fight corruption and improve spending quality. Thus, the Commission proposes to issue a data initiative regarding procurement data, as well as a governance framework. Also, the Data Strategy foresees the provision of guidance on common standards and interoperable frameworks for legal information held at the European and national levels.

- **A Skills Data Space:** The data-driven vision for EU economies requires high-quality data on qualifications, learning opportunities, jobs, as well as on the skill sets of people. In this regard, the Commission proposes to support Member States in the development of digital credential transformation plans and in the preparation of re-usable datasets of qualifications and learning opportunities. Also, in collaboration with Member States and key stakeholders, the Commission will implement a governance model for the on-going management of the Europass Digital Credentials Framework.

2.4. Open Data Directive: access to data held by public institutions

The Open Data Directive (ODD) entered into force on July 16th, 2019, and had to be implemented in national regulation until July 17, 2021. It is the first EU Directive requiring public bodies to make their data open by design and default. Many of the principles defended in the DGA and DA can already be found in the ODD.

The ODD states that access to documents must be free of charge by default and will be granted on request. Member States' public bodies shall take no longer than 20 working days to answer each request. The licenses for the re-use of data will not be subject to conditions unless such conditions are

objective, proportionate, non-discriminatory, and justified on grounds of a public interest objective. Also, data obtained in publicly funded research will be opened or remain in an open-access regime.

The Directive presents the notion of "high-value datasets" which are defined as "documents the re-use of which is associated with important benefits for society, the environment and the economy, in particular, because of their suitability for the creation of value-added services". According to the ODD, these high-value datasets must be available free of charge, machine-readable, provided via APIs, and provided as a bulk download, where relevant. The criteria to classify datasets into "high-value datasets" refer to each dataset's ability to "generate significant socioeconomic or environmental benefits (…) [,] benefit a high number of users, in particular, SMEs (…)[,] assist in generating revenues (…) [,and] be combined with other datasets". Among the sectors are geospatial, earth observation and environment, meteorological, statistics, companies and company ownership, and mobility. The Commission was tasked to propose an implementing act specifying the necessary arrangements for these high-value datasets, which is being developed to this day[7].

The Open Data Directive updates the two previous Directives 2003/98/EC[8] and 2013/37/EU[9]. Taken together, these three Directives gave birth to the Portal www.data.europa.eu. This portal is run by the Publications Office of the EU and currently makes available more than 1.5 million datasets from Member States' public bodies and other international organizations.

[7] The latest draft of the Commission proposal can be found here: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12111-Open-data-availability-of-public-datasets_en.
[8] https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32003L0098.
[9] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32013L0037.

3. Interactions with other EU legal Instruments

3.1. Open Declaration of Digital Rights of 2022

The 2022 Declaration of Digital Rights (DDR) is based on the EU Charter of Fundamental Rights and the EU Treatises' principles (adapted to the digital environment) and shines light on many points declared in the DGA and the DA. Contrary to the latter Acts, the DDR is a recommendation and is not legally binding. The vision enshrined in this document is focused primarily on putting people at the centre of the digital transformation, promoting safe and secure participation, sustainability, solidarity, and inclusion in the digital space, and guaranteeing individuals' freedom of choice in the presence of powerful algorithms and artificial intelligence services[10].

Article 1d) of the DDR states that the EU commits to "actively promot[e] this vision of the digital transformation, also in our international relations". Article 31.2 of the DGA shields any EU organization from being forced by external judicial or administrative decisions to transfer or give access to non-personal data it may hold. Only based on an international agreement shall this transfer happen. The same is stated in the Article 27 of the DA. This clause binds any requesting third country to the political will of the EU and its Member States and forces it to comply with minimum levels of digital security and data protection if it wants to obtain access.

The DA is a clear step for the enforcement of Article 17 of the DDR, "[e]veryone has the right to (…) control (…) how their personal data are used and with whom they are shared". According to the DA, data holders shall "make available to the user (…) data generated by its use of a product" and make this data available to third parties. These DA dispositions match the EU's commitments regarding the privacy of individuals' control over data (Art 17, 18, 19 DDR).

Together with the Open Data Directive, the DGA provides legal support to ensure the enforcement of Article 7b of the DDR regarding digital public services online. Reaching even further concerning the accessibility levels of public data, the DGA helps to guarantee a "wide accessibility and re-use of public sector information".

3.2. Digital Markets Act and Digital Services Act

The EU Data Strategy refers in section 5A that control of data by "Big Tech" will be dealt with in the Digital Services Act package, consisting of both the Digital Markets and Digital Services Acts (DMA and DSA), while the DGA does not mention either of them.

[10] https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733518/EPRS_BRI(2022)733518_EN.pdf.

The Data Act was adopted a few months after the Digital Services Acts package, and thus was designed to work side by side with these two acts. DA recital 10 states that it applies without prejudice to the DSA, and DA recital 36 explicitly mentions the DA's consistency with the DMA. Additionally, Article 5.2 of the DA excludes any entity considered a "gatekeeper" under the DMA as eligible to be considered a third party for data access rights. There is however some uncertainty on this point, in that the DA concerns the data generated by IoT devices, but not derived or inferred data. Additionally, neither the DA nor the DSA package prevent gatekeepers from buying data holding rights or data holders' companies. This is important since the DA seems to prohibit gatekeepers only to acquire generated data from IoT device manufacturers, which may not be the same entity as data holders (CERRE, 2023, p. 18).

3.3. GDPR of 2016, ePrivacy directive of 2002 and ePrivacy Regulation

The DGA is applicable without prejudice to legislation such as the General Data Protection Regulation (GDPR or Directive 2016/679), implying that public bodies must ensure the respect for the nature of re-used data according to the legal provisions in force and by the use of techniques such as anonymisation, generalisation, and randomisation, among others. If the re-use request cannot be granted due to a lack of formal consent, the public body must make its best efforts to support the requester in obtaining the necessary consent from data subjects.

The DA relies on the rules provided by the GDPR framework regarding the processing of personal data and international data transfers and storage. It assumes a complementary and expansionary nature and under no circumstance shall it be applied or interpreted to restrict or limit rights to personal data, privacy, and confidentiality of communications (Recital 7). Likewise, if the GDPR grants a user access to the personal data generated by their use of a device, in the case of a natural person the DA establishes that the "user (…) is further entitled to access all data generated by the product, personal and non-personal" (Recital 30). Also, in situations where the user is not the data subject (enterprises, data traders), the DA mirrors the GDPR's legal requirements, such as the consent of the data subject or legitimate interest.

The proposed ePrivacy Regulation[11] was designed to replace the ePrivacy Directive of 2002. Still under development, the ePrivacy Regulation seeks to protect the rights of internet users, more specifically the confidentiality of their communications. This protection shall cover any form of digital communication, from instant messages, emails, metadata, to cookies and IoT. It has many connections to the GDPR and some to the DA. The ePrivacy Regulation will complement GDPR rules on personal data processing by providing specific rules on electronic communications and therefore will take

[11] https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=CELEX:52017PC0010.

precedence over the latter. As with the DA, the ePrivacy Regulation applies to personal and non-personal data and relies on user consent for the processing of personal data (and the data users generate). However, while the DA gives rights to the users to choose who shall access the data they generate, the ePrivacy Regulation grants individual rights related to the confidentiality of their communications. Furthermore, DA Recital 15 explicitly excludes from its scope many of the ePrivacy-targeted devices: "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". Finally, the ePrivacy Regulation requires user consent to usage by any actor of the data (or metadata) they generate while using an electronic communications service, a service over an electronic communications network or services or networks that are publicly available. For example, this consent shall be required for sending direct marketing communications to the user.

3.4. Proposals for AI Act of April 2021 and AI Liability Directive

The EU has approached the regulation of AI through two recent proposals: the Regulation called "AI Act"[12] and the AI Liability Directive[13]. The proposed AI Act is focused on providing a human-centric, horizontal regulatory framework for the development, placement on the market and use of AI systems in the Union; being a "Regulation" it will apply directly in each member state. On the other hand, the proposed AI Liability Directive establishes legal responsibilities for the use of AI and being a Directive each Member State will have to integrate its dispositions in their national legal framework.

The AI Act shares its policy purpose with other instruments such as the EU Data Strategy and the DGA, while connecting more directly with other instruments. For example, it is explicitly complementary to the DA, via the application of the non-discrimination principle as a mandatory requirement to "minimise the risk of algorithmic discrimination, in particular in relation to the design and the quality of datasets used for the development of AI systems" (AI Act, Explanatory Memorandum, p.4).

3.5. Proposal for Gigabit Infrastructure Act of February 2023

While the proposed Gigabit Infrastructure Act, Gigabit Recommendation and Consultation[14] themselves do not contain references to the European Data Strategy, the impact assessment of the first indicates that high-quality infrastructure is a necessity for the data economy: "The European Data Strategy adopted in February 2020 foresees that the global data volume will reach 175 zettabytes and

[12] https://eur-lex.europa.eu/procedure/EN/2021_106.
[13] https://eur-lex.europa.eu/procedure/EN/2022_303.
[14] https://digital-strategy.ec.europa.eu/en/news/commission-presents-new-initiatives-gigabit-infrastructure-act-proposal.

the data processing model will change to 80% smart connected objects and 20% centralised computing facilities by 2025. The successful and efficient rollout of highly secured and state-of-the-art fibre and 5G networks is therefore indispensable for future digital services and the industrial data wave."

3.6. Intellectual property rights

The DA does not change the legal status of intellectual property rights and trade secrets, with one exception: Databases containing data from IoT devices or related services will not fall under the application of the EU Database Directive (Directive 96/9/EC) to make sure that these databases can be accessed and used under the provisions of the DA. This means that DA databases do not qualify for the sui generis right under Database Directive, which will require its review[15].

Furthermore, the regime of disclosure of trade secrets may be abused via data transfers under the DA. Articles 4(3) and 5(8) of the DA state that "[t]rade secrets shall only be disclosed provided that all specific necessary measures are taken to preserve the confidentiality of trade secrets in particular with respect to third parties", and that "to the extent that they are strictly necessary to fulfil the purpose agreed between the user and the third party and all specific necessary measures agreed between the data holder and the third party are taken by the third party to preserve the confidentiality of the trade secret". Article 8(6) of the DA states that unless if provided by other EU or national law or by DA Article 6, "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" (Trade Secrets Directive). It is clear that the definition and prerequisites of "trade secrets" formulated in the latter Directive will be important for the internal coherence of the DA, as under its Article 8(6) data holders may overclassify important data as "trade secrets" to avoid sharing data.

[15] CERRE (2023, pp. 22-24) and European Commission (2022b).

4. Effects of the European Data Strategy in Three Dimensions

This section addresses the impact and problems of the European Data Strategy in the light of three dimensions: political, economic, and regulatory. We will address each of these dimensions in turn.

4.1. The Political Dimension

The goal of the Communication on the EU Data Strategy (COM/2020/66) and subsequent acts is to make the EU "become a leading role model for a society empowered by data to make better decisions – in business and the public sector." (p.1). Politically, there are various dimensions contained in this goal: first, the EU needs to become more autonomous and a model to other countries and blocks; second, EU societies are expected to grow on data-based and data-driven innovation and on a single market for data with sharing across borders and sectors; third, the two previous points will be based on EU identity and values, namely the role and protection of its citizens' individuals rights, and on market-based competition.

The Commission and its bodies (such as the EDIB) will assume a vital role in the coordination of the data-driven economy. It is important to consider how the EDIB will work. According to the DGA, this body will assume the form of an expert group (Article 29). This group will be composed of dozens of representatives of national competent authorities named under the DGA, the Commission and other EU bodies[16], bodies representing SMEs and other bodies in specific sectors or expertise. The Commission will chair the sessions and have the power to appoint individual experts when required. The role of the EDIB is to advise and assist the Commission to monitor the developments of the provisions of the DGA. It works as a point of contact between the Commission and important stakeholders involved in the process: national competent authorities and sectoral stakeholders (industry, research, academia, civil society, among several others), and its role is to advise the Commission on the development of a "consistent practice" in domains such as data altruism across the Union (art.30, b)) or help in "developing guidelines" on, for example, how to best protect commercially sensitive non-personal data (art.30, d)) or cybersecurity requirements for the exchange and storage of data (art.30, e)).

The existence of the EDIB guarantees a forum between all the relevant stakeholders which is crucial to the success of the transformation proposed in the EU Data Strategy. However, its constitution itself may not be harmonized enough. For example, the DGA states that competent authorities "should be

[16] The European Data Protection Board, the European Data Protection Supervisor, and the European Union Agency for Cybersecurity (ENISA).

chosen on the basis of their capacity and expertise" and if questions regarding compliance with the GDPR arise these entities "should seek (…) an opinion or decision of the competent supervisory authority established pursuant to that Regulation" (recitals 44 and 51). Are there different levels of "capacity and expertise" among Member-States? How will the Commission act when facing repeating dissent in the EDIB?

The Commission's coordination role will be fundamental for the openness or closure of EU data to other economic blocks, such as China or the US[17], and the interaction between EU Member States. This responsibility is clearly stated in the DGA and DA, also, as stated above, by the requirement of international agreements and compliance with minimum levels of data protection for the processing of international data transfers or access to non-personal data held in the EU (DGA recital 22 and article 31; DA Recital 77 and article 27, 2)). Centralizing this coordination should avoid that a divide-and-conquer strategy by outside actors can be successful.

The implementation of the EU Data Strategy will also have consequences for the equilibrium between institutions within Member States, via the requirement to define competent authorities under the DGA and the DA. A lack of coordination between the 27 Member States may lead to a heterogeneous institutional framework and ad hoc adjustments of relationships between public institutions, or even the merger between regulatory entities. This institutional process may significantly delay the full implementation of the EU Data Strategy. A further issue in this respect is the potential for confusion created by the determination of administrative fines and penalties by individual Member States, for which, so far, no guidelines have been set out.

The EU Data Strategy also promotes increasing transparency in the activities of public authorities, with the DGA extending the reach of the Open Data Directive, stimulating the sharing and openness of publicly held data. The promotion of an open data flow from public authorities is also envisioned in the development of other instruments, such as the Public Administration Data Space or in some of the High-value Datasets under the ODD. Internally to the EU, the existence of more horizontal data flows may promote coordination between social actors such as economic groups, political parties, or civil society organizations. The availability of data about EU Member States may also increase local conscience and activism, influencing the governance and policy priorities of cities and urban centres.

4.2. The Economic Dimension

In the economic dimension, the European Commission expects the Data Strategy to have a positive, direct, and horizontal impact on markets by allowing the reuse of data across sectors. In fact, a recent

[17] In May 2023, the European Commission is still analysing the proposed EU-US Data Privacy Framework, with a decision about its "adequacy", clearing the way for free data flows, expected before the summer.

study by the OECD reports that "data access and sharing is estimated to generate social and economic benefits worth between 0.1% and 1.5% of gross domestic product (GDP) in the case of public-sector data, and between 1% and 2.5% of GDP (in a few studies up to 4% of GDP) when also including private-sector data" OECD (2019). The Commission estimates that increasing the availability of data for commercial use and innovation between businesses and empowering consumers and companies using connected products and related services can generate up to 196.7 billion euros a year by 2028[18]. The Commission also estimates that the application of the DA dispositions alone will create up to 2.2 million jobs in the period 2024-2028 European Commission (2022c).

One important component of the EU Data Strategy vision is increased competitiveness and the stimulus to invest in research and innovation. The DGA and DA are meant to create trust for B2B data sharing, but do not actually change the underlying business model or incentives for sharing. Voluntary contributions to sectoral data spaces, in the expectation that the other companies will also contribute, is an invitation to freeriding. Thus, some kind of coordination mechanism seems to be necessary to create mutual commitments to share data, which, considering the experience with network sharing agreements in the electronic communications sector, will arouse the suspicions of competition authorities. Either way, more competition based on shared data will only materialise if there are enough incentives to produce the data to be shared in the first place – while sharing may reduce the incentives to do so competitively.

On the other hand, the DA also contains two propositions that explicitly limit competition of certain types. First, there is Article 6(2)e that prohibits third parties providing aftermarket services from using a data holder's data to develop a competing product or service. This provision attempts to strike a balance between the overall speed of innovation and individual incentives, by protecting the latter while allowing for non-competing innovation. But this comes at the expense of less innovation by third parties. CERRE (2023) refer trade secrets, patents, and copyright protection as alternative means to achieve the same aim. On the other hand, the DA applies to generated data, not to inferred or derived data, which may maintain the incentives for investment in research and innovation. The core idea here is for companies not to focus their resources and business model on keeping data, but rather to create value from transforming and combining data. Lastly, this provision is likely to invite litigation about what "competing products and services" are, leading to legal uncertainty at least until the first cases will have been resolved in court.

In order to balance market power, with Article 5(2) of the DA, the Commission tries to prevent further concentration of data at the gatekeepers denoted under the DMA, by making them ineligible

[18] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13045-Data-Act-&-amended-rules-on-the-legal-protection-of-databases_en.

to access data as a third party from other data holders even upon a user request or if being sub-contracted by the third party (DA, Recital 36). Also with the aim of protecting data holders, this provision reduces data access to some of the most innovative companies and is a limitation to users' right to choose.

Concerning this issue, BEREC (2022) stresses that it is important to address the possibility of gatekeepers bypassing this prohibition by buying data holding rights, instead of the data themselves. This arises from the difference between being the manufacturer of the "data collecting product" and being the data holder of the data generated by this product. Manufacturers can design products to forward collected data to storage other than at its producer's. As of this writing, no agreement on the exact delimitation of the prohibition has yet been reached in the trilogue negotiations. Relatedly, it not immediately clear where to draw the line between the acquisition by the gatekeeper of data rights, data, and the data holder's business itself, with implications for which will be the authority in charge.

SMEs receive special protections under the DA, to lower barriers for accessing data, again with the aim to stimulate competition. First, the DA exempts SMEs from the obligation to make data available to public authorities in cases of emergency, due to its cost. The DA also obliges data holders to limit the compensation asked from a data holder to an SME data recipient, stating that "any compensation agreed shall not exceed the costs directly related to making the data available to the data recipient". Lastly, SMEs will benefit from the contractual fairness clauses of the DA. In its impact assessment, the Commission estimates that the elimination of imbalances in bilateral contractual relations alone can boost SMEs' profits up to EUR 5.2 billion per year European Commission (2022c). Still, CERRE (2022) points out possible problems with this provision: For example, the size of the players involved is not necessarily connected to bargaining power; a position of economic or data dependence may provide smaller players with strong bargaining power.

The cost of compliance with the DA can be another issue. How will the burden to comply affect non-SME companies, and how will it change their behaviour? Will non-EU markets become relatively more attractive or non-EU firms relatively more competitive? Furthermore, the step change in applicable rules and implied investments may create a threshold effect for firms growing up from SME status.

4.3. The Regulatory Dimension

Together with the DMA and DSA, the EU Data Strategy forms part of a movement to set out tighter ex-ante rules for certain markets, instead of relying principally or solely on ex-post intervention by competition authorities. While most of the framework is consistent with competition subject to ex-post enforcement, one clear aim is to avoid competition problems from the start and reduce the

necessity for future intervention, in particular with respect to abuse of market power in bilateral relations. On the other hand, some of the measures, e.g., for voluntary sharing of data, may need closer cooperation between potential competitors, which goes against the grain of present competition policy. As is the case with network investment in electronic communications, finding the right balance may be difficult.

A data-driven Common Market can be expected to lead to further integration of value chains across sectors and Member-States. This may create both synergies in regulation between and the necessity to transform regulatory bodies within Member States, in different but overlapping areas such as privacy protection, competition, or telecoms. Member States may want to create cross-functional working groups drawing on these regulators, emulating the EDIB at national level, or even move towards merging some previously separate regulatory institutions, just as Spain did by merging the competition and telecoms agencies, or Germany by merging all network regulators into the Bundesnetzagentur.

While the EDIB will assist the Commission in implementing the Data Strategy, it remains to be seen whether it will also strengthen the cooperation between regulatory agencies of different Member States. It is also unclear whether any institution will address the social and ethical impacts of data use and related developments in AI under the existing framework.

Additionally, the abundance of work that will result from the DA and DGA will require well-capacitated regulatory bodies. The creation of effective competent national bodies will require a significant investment in human resources and skills, which is will certainly be costly and influence the power equilibrium in public administrations and regulators. The potential for the overlapping of attributions in the areas of privacy, data protection, cybersecurity, network infrastructure, and competition issues may create conflicts.

In establishing these competent bodies, Member States may choose to create new regulatory entities or attribute new responsibilities to the existing ones. In the DA, the Commission gives 12 months to the Member States to do this. BEREC (2022, p. 15-16) mentions the need of permanent dialogue between Member States in this process, and also the possible need to extend this deadline in some cases. It is important to question whether clearer guidelines are needed to harmonize the designation and capacitation of competent authorities.

On May 10th, 2023, the French government unveiled a legal proposal for the digital economy for the protection of users and businesses, including the transpositions of the DSA and DMA and parts of the European Data Strategy (France 2023). The proposal is a good example of the complex web of competent authorities that may arise at national level. Apart from the Competition Authority, the media regulator Arcom will enforce the DSA as “digital services coordinator” and be responsible for

platform content under the DMA (apart from its role of suppressing pornography and hate speech). Also under the DMA, the Directorate-General for Competition, Consumer Affairs, and Fraud Control will oversee marketplaces, while the National Commission on Informatics and Liberty, the privacy regulator, deals with data protection issues. Under the DGA, the latter will also cover data donated in the public interest, the Interministerial Directorate for Digital Affairs will deal with public data, and Arcep, the communications regulator, oversees the data economy and data intermediaries (Euractiv, 2023).

Finally, at the implementation level, CERRE (2023) points out that terms such as "pseudonymisation" and "anonymisation", which are important for the rules about privacy protection, are used inconsistently in the DA. The DA also lacks rules to limit or prohibit problematic data usages such as re-identification and profiling techniques, among others. Even though privacy issues are also being addressed in other EU initiatives (concerning political speech, for example), it is important to remember that many rights enshrined in the DDR could benefit from more specific and stricter dispositions in the DA or any other of the above-mentioned acts, and from clarifications of their relationships in particular with the GDPR. Again, these issues presently are under active discussion in the trilogue negotiations.

5. Impact on stakeholders

The EU Data Strategy and its associated regulatory acts indicate many expected benefits from their implementation, but there are several potential risks as well.[19] We will discuss specific benefits and risks for various kinds of stakeholders, such as individual citizens and users, businesses and SMEs, government and public administration bodies, producers of IoT devices, cloud services providers, national regulatory authorities, research institutions, civil society, philanthropy, data altruism organizations, and countries.

In the rest of the paper, we will present benefits and risks from the point of view of each of these stakeholders. While most of the benefits are related to more transparency, innovation, interoperability, better services and lower market barriers, the risks mainly arise from threats of either insufficient or too burdensome regulatory control and monitoring capacity, possible leaks of personal data, costs of compliance for businesses, and from the remaining uncertainty regarding the practical application of some dispositions of the Data Strategy and its associated acts.

5.1. Citizens/individuals/users

Citizens are at the core of the EU Data Strategy. Directly as well as indirectly, they are the target of the policy. As a direct consequence, expected benefits are more control over the use of personal data and over data generated by IoT devices, as well as benefiting from data-driven innovation. These data may come from an increased range of applications, such as health, education, energy, and transport. Using the example in OECD (2019, pp. 61-62), the reuse of open data released by Transport for London (TfL) generated annual economic benefits and savings of up to GBP 130 million a year for TfL customers, road users, London, and TfL itself. More competition in aftermarket services (especially as a result of the data transfer right enshrined in chapter II of the DA) and the openness of data for free reuse will drive innovation and better services for citizens in key areas such as those mentioned above. These benefits may come as financial benefits, but in the long term may have other forms, such as gains for the environment and overall quality of life.

The Impact Assessment Report of the Data Act estimates that 2.2 million jobs will be created European Commission (2022c), and the EU Data Strategy will make businesses create even more jobs connected to data innovation, governance and protection. Having this in mind, the Commission saw the existing levels in digital skills and data literacy as a potential problem in the EU Data Strategy, promising further investment in this area. This vision is shared among EU institutions and impacts citizens directly. In fact, digital skills, data literacy and the need for education and training are points

[19] For a generic overview of risks in data sharing see OECD (2019, chapter 4).

that stand out in the EP amendments to the Data Act. According to Recital 18a, the EP version of the Data Act reports the need to attract more investment in these two areas from the Commission, the Member-States and all the relevant stakeholders.

Finally, both the EP and the EC show signs of seeing EU citizens' privacy as a cornerstone of the Data Act. The EP, for example, included a Recital clause stating "no provision of this Regulation [Data Act] shall be applied or interpreted in such a way as to diminish or limit the right to the protection of personal data or the right to privacy" and also included a new clause in Article 12 ("Scope of obligations for data holders legally obliged to make data available") stating that "any contractual term in a data sharing agreement between data holders and data recipients which, to the detriment of the data subjects, undermines the application of their rights to privacy and data protection, derogates from it, or varies its effect, shall be void" (EP, Art. 12, 2a).

However, there are several types of risks associated with the implementation of this strategy. The first kind of risks arises from the application of privacy protection and control measures among different actors to prevent unauthorized access or misuse of data. Several parts of the DGA (recital 23; Article 5,5; Article 12, j; Article 21, 4; Article 31, 1) and the DA (Recitals 8, 78; Articles 11, 19, 27) state that the different stakeholders must take appropriate actions to protect and guarantee a safe transfer or handling of data. Moreover, both the DGA and the DA state the need to assure consistency in the internal market's legislative framework, where the same rules should be applied to data handling, guaranteeing similar practices across the Union and fairness in the costs supported by the companies when protecting confidential business data, trade secrets and also personal data[20]. For example, the Commission will present standards for *smart contracts* which should incentivize the homogenization of the guarantees and conditions for sharing data. However, compliance with minimum safety standards for smart contracts is one issue among several others that arise from the freedom of each actor to choose which guarantees to take to accomplish these goals. Some actors may be more diligent, technically more capable or more resourceful than others, and this may create vulnerabilities, namely the danger of involuntary or illegal leakages. Additionally, each Member State will be dependent on its own resources to implement these safeguards with its competent authorities, which again may create different levels of data security (Article 31, 7) and also creates doubts about the varying levels of surveillance capacity of the different competent authorities. Relatedly, each national competent authority shall be nominated according to its experience in areas relevant to the Regulation (such as data protection, competition, electronic communications services) which again is something that may create different levels of expertise among competent authorities. These risks are addressed through

[20] DA, p.7 (2. Legal Basis, Subsidiarity and Proportionality – Legal Basis).

the EDIB and the indication of further regulatory instruments to be adopted by the Commission, but it is not clear if these will work against these risks.

As under the GDPR, repeated authorization requests are cognitively burdensome. Clearly defined formats such as the European Altruism Consent Form may be effective in reducing the burden on users, but only if they are short or pre-filled and without the need for constant interaction. It is hard to expect users to be interested in being data altruistic if this places high demands in time and permanent attention.

5.2. Businesses and SMEs

From the point of view of firms, there are several changes that come with the EU Data Strategy and its Acts. The one obvious benefit will be the access to data. This access will have many realizations. First, firms will be able to reuse data held by EU public bodies and to access high-value datasets and data spaces with data of all Member-States on key areas. Excluding some exceptions (DGA, Article 4, 2) and while protecting trade secrets and confidentiality agreements, firms will be able to access data according to publicly available conditions for such reuse (DGA, Article 5, 1) while paying a proportionate and reasonable fee (DGA, Art. 6, 2).

B2B and B2C data sharing is also addressed through the DA. The access as third parties to data will allow the development of new business models, specifically in aftermarkets services. Data holders will also be able to monetise data by providing access to it, with only some exceptions (SMEs and, possibly, non-profit research organizations). The Council version of the Data Act is also clear about the type of data addressed in the regulatory text: raw and pre-processed data (EC DA, Recital 14a). Of course, this was to be decided in the trilogue, but it is possible that firms that generate value from data transformation (derived or inferred data) will benefit from the DA, especially if they are SMEs (which, according to the DA, will have facilitated access to other firms' raw data).

Other important benefits are expected come from the changes introduced in the rules for switching between cloud services providers (DA Chapter VI). According to the Commission these dispositions will have a positive effect on businesses, reducing "vendor lock-in" effects and allowing companies to pursue a "multi-cloud approach [as] customers of data processing services (…)[,] increasing their digital operational resilience" (EP DA, Recital 69).

The EU Data Strategy considers SMEs as crucial for the functioning of a competitive data-driven EU economy and attempts to strengthen their market position. The DGA states that public bodies shall take measures to incentivize the reuse of public held data by SMEs and start-ups. To that end, the DGA goes further and even suggests that the competent national authorities may supply access at discounted fees or even free of charge (Article 6, 4) to SMEs and start-ups.

The DGA and the DA framework should fight against excessive compliance costs (specially concerning multiple sector companies and DA clause on mandatory free access by public authorities in case of emergencies), the over complexification of data sharing rules and avoid setting arbitrary different compliance regimes to companies with comparable or close market share or dimension (such as SMEs and medium-sized companies). Having in mind this last point, CERRE (2023) questions why the DA only excludes SMEs from DA Chapter 2 obligations (B2B and B2C data sharing) and does not exclude also medium-sized companies (which is, Commission Recommendation 2004/361/EC, companies with less than 250 employees or 50milion of annual turnover). Compliance costs for companies may also rise due to the lack of legal certainty about the process *in loco* of the dispositions mentioned in DA Chapter V: specially those connected to the obligation to share data freely with public entities when facing public emergencies; and the cost-based fees for data sharing in case of public emergencies prevention or mitigation[21]. Although the Commission version of the DA excludes SMEs from these obligations, the Council's version does not and extends those obligations to all companies (SMEs and the rest). To comply with these dispositions may require to all businesses (if the Council's proposal is accepted) or at least to all non-SMEs to incur in infrastructural and operational costs in order to readily comply with DA Chapter V. The EC version does however mitigate these costs in the long term, as its version of Article 20, 1, excludes SMEs from the obligation to provide access to public authorities free of charge.

DA Chapter 4 is dedicated to unfair terms related to data access and use between enterprises. Its Article 13 is dedicated to SMEs and, according to its first clause, "a contractual term (…) which has been unilaterally imposed by an enterprise on a [SME] shall not be binding on the latter enterprise if it is unfair". The European Council version applies these fairness clauses to all enterprises and not only to SMEs. However, in its initial version, the "fairness" tests laid down in the following clauses of Article 13 all give bargaining power to SMEs (in terms of contract negotiation and interpretation, each part's liability, among other points).

Contrary to access for larger businesses, the compensation paid to data holders for data access by SMEs cannot exceed the cost of providing the data. The definition of these costs is still unclear. Certainly, these costs will be later specified either through the revision of the DA in the trilogue or in further decisions by the Commission. We do know that the current interpretation of the EC about these costs is that these must reflect "the cost necessary for the formatting of data, dissemination via electronic means and storage" (EC DA, Article 9, 1, a, a)). On this matter, the EP leaves the definition of the "costs directly related to making the data available to the data recipient and which are

[21] From the perspective of the National public authorities, please see subchapter 5.9: Public Authorities.

attributable to the request" (EP DA, Article 2) to the Commission to later develop "guidelines to determine criteria for categories of [these]" (EP DA, Article 2a).

Furthermore, the Commission's DA proposal indicates that SMEs will not be legally obliged to have a data structure to assure public access to their data in public emergencies. This is yet to be defined, as the EC does include this obligation for SMEs under specific conditions (EC DA, Article 15, 1, a).

Some of the potential risks are related to gatekeepers under the DMA. Curiously, one expected benefit may pose risks: the "unfairness" test of Article 13 mentioned above. According to this test, a contractual term is to be considered unfair if it "grossly deviates from good commercial practice in data access and use, [is] contrary to good faith and fair dealing". CERRE (2023) notes that these terms could act as a straitjacket for contractual B2B relations. DA Recital 54 serves to balance this, saying that "[c]riteria to identify unfair contractual terms should be applied only to excessive contractual terms, where a stronger bargaining position is abused" and that "[t]he vast majority of contractual terms (…) are commercially more favourable to one party than to the other, including those that are normal in business-to-business contracts, [they] are a normal expression of the principle of contractual freedom and shall continue to apply". Even with all the clauses included in the rest of the Article, it is not clear when "commercially more favourable" contractual terms come to deviate from "good commercial practice in data access" or "contrary to good faith and fair dealing". How will this balance be applied across all EU Member States? The EU Council version adds a retroactive clause, namely stating that "[b]usinesses shall be given three-years following that date to review existing contractual obligations that are subject to this Regulation" (Article 13, 8a). Another part of the DA's treatment of gatekeepers (mirrored in article 5.2 and article 6.2d) may also work against one of its primary objectives (to foster innovation) by prohibiting third-party data sharing with gatekeepers. CERRE (2023) notes that the role gatekeepers have in producing connected products or data-generating services is often considerable and makes them experienced providers of aftermarket services. If controls are set correctly to limit the overpowering reach of gatekeepers to customers when compared to other players' capabilities, the entrance of gatekeepers in certain markets can indeed further incentivize innovation. Examples of these controls to limit gatekeepers from excluding other actors from markets are those mentioned in DA article 5.2a and b, not allowing to "solicit or commercially incentivize a user (…) to make [his/her] data available [or to request the data holder to make [his/her] data available] to one of [the gatekeepers'] services".

Furthermore, the DA expressly includes trade secrets in its data sharing obligations. This can have a negative effect if we consider companies operating worldwide and not only inside the EU. The DA has several clauses (recital 28, 66, 77; Art. 4.3; Art. 5.8; Art. 17.2c; Art. 19.2) that explicitly state that data holders may require the protection of data that may contain trade secrets, property rights, etc,

through contractual agreement with users and third-party data recipients. Beyond this, the DA prohibits third parties who access this data from using it to produce or develop any competing product or service (Art. 6.2e). This point is important if we consider that some businesses will lose market power or competitive edge (built on their data superiority) if they are obliged to share data with rivals, making the protection provided by this article crucial to these companies' existence and activity. However, we must not forget that the jurisdiction of the Data Act is the EU, so it remains to be seen how these clauses can have any effect outside the EU. In other words, it remains unclear how the lack of jurisdiction of the DA outside the European space will affect EU companies' competitiveness outside the EU. In such cases, DA Chapter VII may not protect EU companies. Take the case of German company Siemens, which addressed a revision request to the Commission precisely because of this risk[22].

There is a risk that third-party business models as envisaged by the DGA and DA will not work because not enough users request to transfer their data. If this is the case, part of the vision of the EU Data Strategy will fail to materialize. Take the case of aftermarkets services. It is not clear if there will be enough users requesting data transfer to any of these companies both because of the additional time required of the user to make that request and because diverging user preferences may imply a fragmentation of the market for aftermarkets services – if firms there do not reach a critical mass of users they will not be commercially viable.

5.3. Civil society and Data Altruism

Civil society organizations will likely benefit from data openness. More publicly available data provide a clearer view for addressing societal needs, which can better direct the actions of philanthropists and non-governmental organizations. Also, common or activist causes, such as for EU consumers rights or environmental protection, may increasingly assume an international form, as relevant data on all EU Member-States is made available in central repositories.

However, civil society organizations and non-profit organizations will assume a crucial role in data altruism. According to the DGA, the label of "data altruism organizations" (DAOs) aims to promote cross-border data access, as well as the creation of data repositories (DGA, recital 46). Portals such as PORDATA (Portugal) or Statista (Germany) are expected not only to reformulate their business model (in the cases where there is a business model), but also to increase their data offer. According to the DGA, this type of institution will be certified as DAO, which will entail a regulatory oversight framework that did not exist before, but that may also attract more actors. It is however unclear which are the

[22] https://www.reuters.com/technology/siemens-sap-say-eu-draft-data-act-puts-trade-secrets-risk-2023-05-07/

implications for data providers that do not register as DAOs or use this label. It is important to note that fines or penalizations against these actors may work against the goal of promoting data altruism.

5.4. Producers of IoT devices

IoT producers will benefit if a many new players are created to provide aftermarket services for their products. In this case, producers can focus their resources on the production and development of products and leave secondary services (such as repair) to other minor actors.

The anti-competition clause in the DA (Article 6, 2, e) prohibits the use of data by third parties to develop competing devices. This meant as a protection for IoT producers, but may limit innovation.

One risk for IoT devices manufacturers concerns IoT companies' business models. That is, if their business model is based on the exclusive propriety of the data their products/services generate, it is clear that if they have to let go of these data, these companies must rethink their way to produce value. Under the DA, additional costs will arise from transferring or allowing access to the generated data to requesting users or authorized third parties. Complying with the DA will certainly require investment in IT infrastructure and staff.

5.5. Providers of cloud services

The EU Data Strategy aims to reduce lock-in where costumers of cloud and data service providers cannot move to other providers due to contractual obligations, lack of interoperability, or cost of switching. The DA states that "After a transition period of three years after this Regulation enters into force, all 'switching charges' should be abolished" (Recital 72, b). The EC version of the DA declares that no data egress charges or switching charges will be imposed on customers for any switching processes (art. 25, 1). Providers must reduce charges to their customers to the "costs incurred by the provider of data processing services that are directly linked to the data transfer and the switching process concerned" (art. 25, 3).

These provisions do not only benefit the customers of cloud and data services providers, but also make this market more contestable and invite entry of new providers. Evidently, at the same time these provisions create the possibility of higher churn for the same new providers, which probably implies that these providers will have to subsist with lower margins than the existing large providers that until now have been protected by barriers to switching.

Cloud service providers will be prohibited from erecting any "commercial, technical, contractual and organisational obstacles" that may have a "vendor lock-in" effect (DA, Article 23). Article 24 of the DA provides additional "contractual terms concerning switching between providers of data processing services", namely the need of a written contract which must define the clauses under which the

customer may request "to switch to a data processing service offered by another provider (…) or to port all data (…) generated directly or indirectly by the customer to an on-premise system, in (…) a mandatory maximum transition period of 30 calendar days" (Article 24, 1, a)). Additionally, the Commission declares the gradual remission of switching charges during the first 3 years after the entry into force of the DA (Article 25). After that, no switching charges shall be applied.

On the other hand, these provisions, by making customer churn easier, also increase competitive pressure on the hoped-for European entrants in the cloud services market. Whether this outweighs the potential gains from being able to capture clients from the large incumbents is unclear, but may certainly imply that European providers will not be able to grow easily to similar size.

5.6. National Regulatory Authorities

From the point of view of national regulatory authorities, the DA and DGA will change national equilibria of power and attributions. While some of the existing agencies may gain new responsibilities, other agencies may be created. This provides an opportunity to reorganize the network of regulatory agencies in each Member State, in particular with respect to those whose attributions gain a stronger overlap in the digital economy. Also, EU-level platforms such as the EDIB will promote the dialogue between national regulators on data and can help to harmonize regulatory proceedings. New competencies over data and its governance will most likely allow for more ex-ante control over the markets and competition, reducing the necessity for ex-post interventions of competition abuses.

There will be a clear necessity for Member States to provide more resources and staff to their agencies, in order not to threaten the effectiveness of the data regulation framework through an insufficient regulatory capacity of already overstretched institutions. Another important risk, if not properly addressed in the design and distribution of tasks, is the possibility of overlaps in jurisdiction between national regulators of different areas.

5.7. Research institutions

A direct impact of the EU Data Strategy on research institutions will be through the European Open Science Cloud (EOSC). The EOSC did not start with this communication in 2020, but was first mentioned in 2015, in the Commission's *A Digital Single Market Strategy for Europe* (COM(2015) 192 final)[23]. However, it is envisioned in the EU Data Strategy as a part of the EU data spaces environment. To further integrate the EOSC in this environment, the Commission committed to continue to implement the EOSC, namely promoting the participation of the public and private sectors. This participation has

[23] Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52015DC0192.

taken place under the current tripartite governance which comprises the Commission, representatives of Member States and Associated Countries, and key stakeholders in the area of research. The EOSC will exist as a space modelled by commons standards of governance and data quality (FAIR principle: "Findable, Accessible, Interoperable and Reusable") where publicly funded research outputs are openly available, and where EU researchers can publish, find, and reuse data, publications, software, tools and services for scientific and research purposes. As such, the EOSC will certainly require EU research institutions and researchers to comply with rules and quality standards agreed on by its three-fold governance. Possibly, complying with the EOSC's rules may in the future imply more actions from these institutions, for example, the professionalization and integration of "data stewards" in each organization's structure[24].

On the other hand, the Open Data Directive (ODD) is the core regulation affecting the openness for academic research. However, the ODD is directed only towards public sector bodies, leaving out of this open environment private undertakings. The DGA and the DA add new standards and expected practices to amplify the open regime for research, but also include the application of terms and conditions (to protect sensitive data) for the reuse (DGA), as well as of technical protection measures and smart contracts (DA, recital 24).

A recent study by the European Commission (2022a) of the impact of these two acts on research institutions reports some possible setbacks regarding the application of the EOSC. One of them is the probable legal entanglement with other jurisdictions beyond the EU. These entanglements are mainly related to issues such as (contractual) rights of users of services, data protection law or export controls of sensitive knowledge. Also, one should note that joint ventures on research between private and public actors are out of the scope of the DGA (recital 12). Unless each Member State addresses this issue, this "gap" may prevent the full potential of opening all publicly funded data to be realized. Probably, some kind of coordination will be required to address different levels of openness in public data across Member-States. Additionally, issues relating to the fundamental right to academic freedom may arise, namely the freedom of researchers to have a word on where and for what purposes their data and research outputs will be (re)used.

5.8. Public Administration

One crucial benefit envisioned in the DA is the creation of a legal framework that establishes the obligation to make data available to public authorities in case of public emergencies (take the case of

[24] See https://www.prometheusnetwork.eu/blog/the-european-open-science-cloud-and-its-crucial-guardians-the-data-stewards/

public health emergencies or major natural disasters) or in situations where public sector bodies have an exceptional need to use certain data.

This will of course put strong pressure on all EU public authorities to comply with the requirements from the EU Data Strategy. For example, for more transparency and comparability to result from the application of common standards across EU public authorities when feeding their EU data space, it is not reasonable to think that each of these public authorities presently have the same resources or capacities to comply with these data standards. The need for additional resources for ends of transparency is not only limited to the EU data space for public authorities. For example, DGA Art. 9 stipulates that public authorities must answer to a reuse request in under 2 months following that request. This period may be shortened under national law. The DGA also will require urgent action of public authorities on its exclusive arrangements (DGA Art. 4). Exclusive agreements on the reuse of publicly held data (DGA Art. 3.1), out of the scope of two exceptions (Art. 4.2 and 3) and that "were concluded before 23 June 2022[,] shall be terminated at the end of the applicable contract and in any event by 24 December 2024". Furthermore, public authorities must "make publicly available the conditions for allowing such re-use and the procedure to request the re-use" (Art. 5). These are a few examples of the additional workload envisioned for EU public authorities which makes one wonder whether the existing different levels of budgetary capacity (even if that capacity is legally guaranteed in DGA Art. 7.3,[25] is it not reasonable to consider that the outcome may vary substantially between Member States?), "data readiness" or digitalization across EU public authorities will be sufficient, or whether there will be a risk of noncompliance in some countries.

One potential risk is related to the situations where this access must be granted for free (Article 15, a): to respond to a public emergency) and when it must result in fair compensation (Article 15, b), c): to prevent/recover from a public emergency). This compensation shall not exceed the technical and organisational costs incurred to comply with the request (Article 20, 1). However, will there be incentives for public authorities trying to access data only when it is free? That is, granted that compensation now is written into the DA text and must be paid, will public authorities try to minimize their expenses on data access fees by stretching the notion of "response"? Moreover, DA Recital 57 reports that "the existence of a public emergency is determined according to the respective procedures in the Member States (…)" which may differ substantially across Member States.

Member State and EU public administrations will also be responsible for feeding the Public Administration data spaces which, according to the EU Data Strategy, are expected to make data for areas such as public procurement, law, and public spending comparable (in close collaboration with

[25] "The competent bodies shall have adequate legal, financial, technical and human resources to carry out the tasks assigned to them, including the necessary technical knowledge to be able to comply with relevant Union or national law concerning the access regimes for the categories of data referred to in Article 3(1)."

the Member States, the Commission promised to issue guidance on common standards as well as interoperable frameworks for legal information) and accessible on “findable, accessible, interoperable and re-usable” (FAIR) terms. The need to integrate public administration data at EU level may also work as an incentive for the digitalization of public services.

5.9. Countries

The EU Data Strategy is designed to bring several benefits to EU countries. Interoperable data, a single market for data, greater transparency, public authorities’ access to data under exceptional need are stipulated. The EU Data Strategy also represents the definition of a standard baseline for important public tasks such as data interoperability requirements, minimum data collection necessities for public authorities, standardized procedures to promote an integrated single market (DGA obligations, EU consent form) and designates supporting bodies, such as the European Innovation Board and competent authorities. All these benefits respect essential core values assumed by the EU and its Member States, which harmonizes and reinforces Member States’ relations and actions on the international scene.

As with the other relevant stakeholders, the EU Data Strategy and its acts bring risks to EU countries that are important to be aware of. The first risk concerns countries’ local businesses. The DA and the DGA include several legal protections for SMEs and start-ups, which are two forms of many EU local businesses. However, there are two types of risks associated with the implementation of these acts that most likely will not be eliminated by these protections. The first type is related both to the concrete application of the DA, that is, will local businesses be aware of the protections meant for them? Will they use them effectively? Will national competent authorities be capable of addressing all their data requests or cries for help? How accessible will be these legal protections? The second risk stems from the proper functioning of the markets after the implementation of the acts, namely network effects such as market concentration, limited access to capital for local businesses to invest in data infrastructures and digital skills shortages, which can significantly influence SMEs' ability to innovate and affect their integration in EU markets. Local businesses may find it financially overpowering to invest in capabilities to comply with the DGA or the DA, to reskill their human resources, or to attract this type of skills. Furthermore, compliance costs may strain funds previously allocated to innovation.

Moreover, innovation value creation may become concentrated in some Member States or regions, leveraged by market-level or ecosystem-level network effects and starting from the already large differences between Member States’ economies.

Although the DA is a Regulation, applying directly in Member States, and not a Directive that must first be transposed into national law, countries still have plenty of room to differ in its implementation. It is in this context that risks may arise, for example in the setting of fines and interpretations of legal concepts such “unfair contractual terms”.

Furthermore, if access to data from all Member States and EU companies becomes more open, innovation and value concentration may become concentrated in a few Member States as a consequence of more attractive enforcement policies. This concentration can also be fuelled by different enforcement and penalties applied in each Member State. According to DA Article 31, Member States shall “designate one or more competent authorities as responsible for the application and enforcement of this Regulation”. DA Article 33 also says that Member States shall “lay down the rules on penalties applicable to infringements of this Regulation” which must be “effective, proportionate and dissuasive”. However, this is not enough to guarantee that a Member State’s enforcement of the DA can become more “attractive” to actors that expect to stretch the limits of the law. In this scenario, companies may avoid stricter Member States for softer ones.

There is also a risk that arises from the different levels of resources and capabilities of national competent authorities to monitor compliance with the DA in their territory. Member States with less monitoring capacity and with slower legal systems may attract more DA *noncompliant* companies, which may overwhelm these Member States’ legal and public authorities even more.

Finally, disagreements between Member States and the European Commission are not a recent phenomenon. This brings up two general risks the EU Data Strategy may represent: lack of solidarity between Member States and the misalignment of geopolitical priorities. Just to mention a few examples, there are the 2017 Polish reforms of the judicial system or the Nord Stream 2 agreement between Germany and Russia in 2015. Both the DGA and the DA allow for international transfer of data under international agreements celebrated both between third-party countries and the Commission or between these countries and EU Member-States. It is clear that the EU Data Strategy vision for a data economy grounded on EU values will only survive when these same EU values are shared among all 27 Member States and their protection is pursued by all of them.

References

BEREC. (2022). *BEREC High-Level Opinion on the European Commission's proposal for a Data Act.*

CERRE. (2023). *Data Act: Towards a balanced EU data regulation.* CERRE. Obtido de www.cerre.eu

Euractiv. (10 de May de 2023). *France mulls new 'frontline' digital bill going beyond EU rules*. At https://www.euractiv.com/section/platforms/news/france-mulls-new-frontline-digital-bill-going-beyond-eu-rules/

European Commission. (2022a). *Study on the Open Data Directive, Data Governance and Data Act and their possible impact on research.* Publications Office of the Europ

ean Union. At https://op.europa.eu/en/publication-detail/-/publication/a313139b-1147-11ed-8fa0-01aa75ed71a1

European Commission. (2022b). *Study to support an impact assessment for the review of the database directive.* At https://copenhageneconomics.com/wp-content/uploads/2022/02/study-to-support-an-impact-assessment-for-the-review-of-the-database-directive.pdf

European Commission. (2022c). *SWD(2022) 34 final: Impact Assessment Report accompanying the document Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act).* Brussels. At https://digital-strategy.ec.europa.eu/en/library/impact-assessment-report-and-support-studies-accompanying-proposal-data-act

France. (2023). *Dossier de Presse: Sécuriser e réguler l'espace numérique.* At https://www.entreprises.gouv.fr/files/files/secteurs-d-activite/numerique/dp-pjl-securiser-et-reguler-lespace-numerique.pdf

OECD. (2019). *Enhancing Access to and SHaring of Data: Reconciling Risks and Benfits for Data Re-Use Across Societies.* Paris: OECD Publishing. doi:https://doi.org/10.1787/276aaca8-en

IPP POLICY PAPER 25

European Data Strategy: Regulatory & Policy Aspects

Authors: Steffen Hoernig and André Ilharco

ISSN: 2183-9360

July 2023

INSTITUTE OF PUBLIC POLICY

LISBON

Institute of Public Policy Lisbon – Rua Miguel Lupi 20, 1249-078 Lisboa PORTUGAL

www.ipp-jcs.org – email: admin@ipp-jcs.org – tel.: +351 213 925 986 – NIF: 510654320