CLUSTERING COMMERCIAL OBSTACLES IN THE EUROPEAN DATA LEGISLATION

Maximilian Gartner / Dino Girardi / Monica Palmirani

PhD Researcher, KU Leuven, Sint-Michielsstraat 6 box 3443, 3000 Leuven, Belgium / University of Bologna, CIRSFID – ALMA AI, Via Galliera, 3, 40121 Bologna, IT, maximilian.gartner2@unibo.it

PhD Researcher, University of Bologna, Via Zamboni 33, 40126 Bologna BO, IT / Lapin yliopisto, Yliopistonkatu 8, 96300 Rovaniemi, FI, dino.girardi@unibo.it

Full Professor, University of Bologna, CIRSFID – ALMA AI, Via Galliera, 3, 40121 Bologna, IT, monica.palmirani@unibo.it

Keywords: ***DGA, DSA, GDPR, Data Act***

Abstract (EN): *As businesses fall under increasing amount of digital legislation, compliance becomes more complex. This article compiles the main administrative hurdles businesses are required to comply with under the European data legislation (General Data Protection Regulation, Data Governance Act, Digital Service Act and the Draft Data Act), and identifies four clusters of requirements that are imposed on businesses throughout these legal instruments: information provision requirements, infrastructure and capacity requirements, market power-balancing requirements, and governance requirements. Drawing from this novel perspective, the paper outlines an aggregation of commercial obstacles that derive from the administrative overhead imposed by such requirements.*

Abstract (DE): *Für Unternehmen ist die Beachtung der steigenden Vielfalt europäischer Gesetzgebung im digitalen Bereich komplex. Dieser Artikel analysiert die großen administrativen Hürden für Unternehmen, die sich durch die Datenschutz-Grundverordnung, den Data Governance Act, den Digital Service Act und den Data Act ergeben, und stellt diese in vier thematischen Gruppen dar: Informationsfreigabepflichten, Infrastruktur und Kapazitätsbereitstellungspflichten, Marktmacht-Balancierungspflichten, und Unternehmensführungs- und Governance-Pflichten. Von dieser neuartigen Perspektive ausgehend identifiziert dieser Artikel fünf potentielle negative Folgen für Unternehmen die durch Beachtung der gegenständlichen Gesetzgebung herbeigeführt werden droht.*

1. Introduction

The digital landscape is evolving rapidly, and businesses are facing growing challenges to remain compliant with the rules shaping the European Market. These changes to regulation are rooted in the European Strategy for Data. One of the main goals of this strategy is to ensure competitiveness of the European market vis-à-vis other global leaders such as the USA and China.[1] Within this approach, taking into account the complex composition of different interests from different stakeholders acting in the digital domain, the European Strategy for data is two-pronged: First, the interests of European citizenry is paramount as is visible in the focus on protection of fundamental rights, the drive towards open government data and the enforcement of data

[1] See e.g. the following quote: "The EU has the potential to be successful in the data-agile economy […] However, competitors such as China and the US are already innovating quickly and projecting their concepts of data access and use across the globe. In the US, the organisation of the data space is left to the private sector, with considerable concentration effects. China has a combination of government surveillance with a strong control of Big Tech companies over massive amounts of data without sufficient safeguards for individuals. In order to release Europe's potential we have to find our European way, balancing the flow and wide use of data, while preserving high privacy, security, safety and ethical standards.", COM(2020) 66 final, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52020DC0066.

sovereignty principles. Second, there is an attempt to protect and support businesses, and in particular SMEs, by ensuring a healthy and competitive market.

These approaches come with a substantial set of regulation, applicable not only to major market players but any business that engages in the digital domain. The increasing complexity of these requirements imposes significant administrative overhead; this translates into commercial obstacles for businesses. In this paper we provide an overview over of the main administrative hurdles imposed by European data legislation and identify four clusters in which these obstacles can be distinguished. To this end, we consider both existing and upcoming European legislation. Based on these findings we suggest five main implications for businesses and their commercial activities. Finally we briefly contrast these with European initiatives meant to shape the European market in favour of commercial actors.

2. Overview over the European Data Legislation

In this paper we investigate four of the major European data legislation instruments. Each of these complement the legal landscape at large, extending harmonising regulation onto different sectors of the data economy. Most broadly, we can assign different purposes to the particular regulations. The General Data Protection Regulation (GDPR)[2] deals primarily with the processing of personal data, the rights of the data subjects and the requirements that are imposed on the entities that partake in such processing.[3] The Data Governance Act (DGA)[4] introduces regulation in three distinct areas: re-use of public sector data, supervision of data intermediation services and data altruism collection for disclosing individual personal data for general interest.[5] In this, the DGA follows the Open Data Directive, aiming to facilitate secondary reuse of personal data voluntary contributed by data subjects for supporting public purposes.[6] The Digital Service Act (DSA) primarily imposes regulation on the provision of intermediary services, by establishing a liability framework and creating due diligence obligations for certain providers. Lastly, the Data Act (DA)[7] aims to regulate and harmonizes the availability of data generated by certain products (e.g. IoT-devices), and to ease switching between different providers of data processing services. The DA also create mechanisms for public bodies to access data of (large) businesses in for "exceptional need". Seen in aggregate, the European Strategy for Data's approach seems to be both intended to combat dominant market positions of entrenched companies as well as empowering everyone else (including SMEs and public entities) through opening of data silos and enabling re-use of data, accompanied by protective provisions for stakeholders with limited market power.

It is often useful to understand that these instruments exist not in a vacuum but in a complex interplay within each other. The DGA and DA originate from the European Commission's European Strategy for Data,[8] while the DSA was announced together with its competition-law counterpart, the Digital Market Act. The GDPR

2 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC http://data.europa.eu/eli/reg/2016/679/oj.

3 While out of this scope for this paper note also the importance of the 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, which intends to create the "European Single Digital Market" in conjunction with the GDPR. This regulation is light in compliance requirements that apply to most businesses and is hence not included in the present analysis.

4 Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) http://data.europa.eu/eli/reg/2022/868/oj.

5 Data altruism is outside the scope of this paper, as it is not a commercial undertaking.

6 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 http://data.europa.eu/eli/dir/2019/1024/oj.

7 Proposal for a Regulation of the European Parliament and of the Council on harmonized rules on fair access to and use of data (Data Act) [2022] COM/2022/68 final.

8 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 COM (2020) 66 Final' https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066.

acts almost as a precursor, which, at the time, pioneered the now more common wide-ranging regulation of the digital domain, including significant enforcement mechanisms.[9] This is relevant in particular as after the introduction of the GDPR, many of these legal instruments were developed in parallel and in explicit knowledge of each other. As the regulations have undergone the processes of European legislation, they have been increasingly harmonised with each other as well. Recognizing this, it is useful to understand the European data legislation as a compound legal instrument in progress. The analysis undertaken in this paper recognizes and confirms this by identifying common regulatory approaches beyond single legal instruments.

3. Legal Denominations of Businesses in the Data Economy

Insofar businesses (or their legal personas) use and process data or otherwise engage in the data economy, they invariably fall within the scope of the European data legislation. The general approach of these regulations is to assign a legal status to businesses that engage in certain data-related behaviour (e.g. the status as data processor or data recipient), and then assign legal obligations to those denominations. This section briefly introduces the most important of these legal denominations for clarity through the lens of businesses and their commercial behaviour.[10]

Introduced by the GDPR and of utmost practical importance is the status as *data controller* used for entities that determine the purposes and means of processing[11] of personal(!) data,[12] and *data processor* for their subsequent subcontractors.[13] The counterpart to these entities within this regime is the *data subject*. Both the DGA and the DA use the terms *data holder* and *data user*. Businesses are *data holders* if they have the right to grant access to or share (non-)personal data.[14] Conversely, businesses are *data users* if they have lawful access to certain personal or non-personal data and have the right to use that data for (non-)commercial purposes.[15] Additionally, the DGA also introduces the notion of a *data intermediation services provider* (DISP), which describes businesses that engage in data intermediation services, i.e. services that aim to establish a commercial relationship for the purposes of data sharing.[16] Conversely, the DA introduces the concept of *data processing services provider* (DPSP), *data recipient*,[17] and *operators of data spaces* (ODS).[18] The first describes businesses that provide services that on-demand administration and broad remote access to a "scalable and elastic pool of shareable computing resources or a centralized, distributed or highly distributed nature (e.g. cloud computing).[19] The second describes entities to which a data holder makes data available for their commercial use.[20] This includes businesses that act as *third parties*, for which the data transfer occurs based on a request of the product or service user. Finally, the DSA creates harmonised rules for the provision of

[9] See for a general discussion on the impact of the GDPR as arguably the first of its kind e.g. Michael Kretschmer, Jan Pennekamp and Klaus Wehrle, 'Cookie Banners and Privacy Policies: Measuring the Impact of the GDPR on the Web', *ACM Transactions on the Web*, 15.4 (2021), 1–42 https://doi.org/10.1145/3466722; Samuel Greengard, 'Weighing the Impact of GDPR', *Communications of the ACM*, 61.11 (2018), 16–18; Paul Breitbarth, 'The Impact of GDPR One Year On', *Network Security*, 2019.7 (2019), 11–13.

[10] As a result, this means that all definitions are formulated as if they reference a commercial entity. Note that this is not a necessity under the European Data Laws.

[11] Whereas data processing describes "any operation on personal data (e.g. collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction)", see Art. 4 (1) GDPR.

[12] Art. 4 (7) GDPR.

[13] Art. 4 (8) GDPR.

[14] Art. 2 (8) DGA.

[15] Art. 2 (9) DGA.

[16] Art. 2 (8,11) DGA.

[17] Note that the DSA uses a very similar definition for the term *trader*.

[18] Note that the DA does not define this term.

[19] Art. 1 (1) e, Art. 2 (12) DA.

[20] Art. 2 (7) DA.

so-called intermediary services, i.e. *hosting*, *caching* and *mere conduit*-services[21] within the Union market, in part by creating rules on due diligence obligations for such *providers of intermediary services* (PIMS).[22] Certain providers of hosting services are also denoted as *online platforms* or *search engines*.[23] Within this regime, additional provisions apply to *providers of very large online platforms* or *online search engines*.

4. Regulation Clusters in the European Data Law

Within this paper we analyse the regulations through which the European Data Laws impose commercial obstacles (e.g. due to them imposing additional administrative effort for businesses) in aggregate, i.e. by considering the general motivation and purpose of a given provision. We suggest that there are four clusters (or super-types) of provisions that affect businesses by imposing commercial obstacles and that these types ought to be understood as transcending a single legislative instrument. As a result, this paper proposes a novel grouping of such provisions and their respective obstacles to better formalize the interdependencies and shared purpose behind such regulative attempts. Broadly, we propose understanding the regulatory landscape introduced as a bundle of obligations for businesses that can be divided into the following clusters: information provision requirements, market power balancing requirements, infrastructure and capacity requirements, and governance requirements (including data limitation requirements). Figure 1 provides an overview over these clusters and their subsets of requirements. This section will explore these clusters in turn to highlight their cross-sectoral nature.

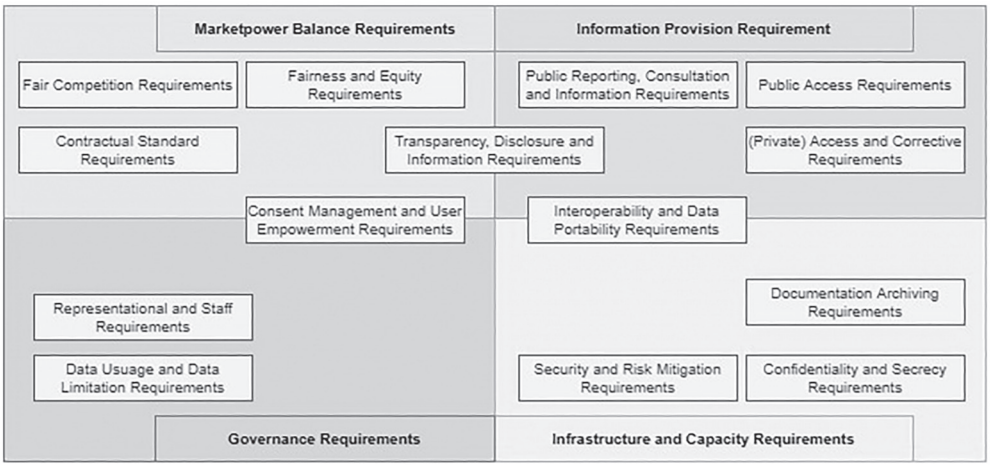

Figure 1 – Clusters of Legal Requirements for Businesses in the Data Economy

[21] Note here that both the DSA and the DGA deploy very similar terminology for different purposes. Under the DSA a *provider of intermediary services* provides so-called "information society services", i.e. conduit, hosting or caching services. Under the DGA, data intermediation services providers offer services 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, through technical, legal or other means, including for the purpose of exercising the rights of data subjects in relation to personal data" (with some exceptions). See Art. 2 (11) DGA, Art. 3 (g) DSA.

[22] Art. 1 para 2 lit a DSA.

[23] Art. 3 lit i DSA. Note the varying language in the DSA as the definition maps the term online platform to a "provider of a hosting service", while later provisions talk about "providers of online platforms".

4.1. Information Provision Requirements

Generally, businesses can freely decide what type of information they share with a wider audience and may sometimes even be barred from "oversharing" information for the protection of their shareholders' value. However, this general principle is overruled in cases where private and public entities are (for different reasons) entitled to obtain information from the businesses. Within this cluster of obligations we can differentiate further.

First, we turn to regulations that mandate businesses to report information or interface with the relevant authorities without any investigative probing. These regulations typically relate to disclosure of breaches, compliance with requests of authorities or notifications when ceasing services or acting against illegal content.

Table 1 – Public Reporting, Consultation and Enforcement Requirements

Data Controller	DISP	PIMS	Provider of very large Online Platforms / Online Search Engines
Art. 33, 36 GDPR	Art. 11, 14 para 3,4 DGA	Art. 7, 9,10, 15 DSA	Art. 24, 42 DSA

Second, European legislation gives public entities unique privileges that allow them access to a company's digital information. Companies must be equipped to provide the necessary information in the prescribed modality (or requested modality).

Table 2 – Public Access Requirements

Data Holder	Data Controller / Data Processor	Provider of (very large) Online Platforms / Online Search Engines
Art. 15, 18 DA	Art. 58 para 1 lit a, e GDPR	Art. 40 DSA

Connected to the rights of entities affected by the data processing by businesses, the European legislator has installed obligations to allow interested parties to access, restrict use or correct the businesses' data processing operations.

Table 3 – (Private) Access and Corrective Requirements

Data Controller	Data Holder	Hosting Provider	Online Platform Provider
Art. 15–18 GDPR	Art. 4 para 1 DA	Art. 16 DSA	Art. 22 DSA

Sitting between the present cluster and the later outlined cluster of infrastructure and capacity requirements, regulations to combat data silos and ensure competitiveness have been given increased weight in recent legislation. The European legislator has been pushing strongly towards standardization and consequently improved interoperability and data portability for some time and not just for personal data. Many of these obligatory developments were also reflected in the Regulation on a framework for the free flow of non-personal data in the EU.[24] For companies, this requires staying abreast of the state-of-the-art and either incorporate data into their workflow in a standard format or develop processes which translate between proprietary formats and an interoperable standard. It is noteworthy that the European Commission is expected to provide guidelines on relevant interoperability standards.[25]

[24] See e.g. Article 6 of the 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. Note that many of the encouragements or self-regulatory aspects of this instrument have now become mandatory through subsequent regulations.

[25] See e.g. Article 22 lit d DGA, Art. 29 para 6 DA (Draft).

Table 4 – Interoperability and Data Portability Requirements

Data Controller	DISP	DPSP	ODS
Art. 20 GDPR[26]	Art. 12 lit i, d DGA	Art. 26 DA	Art. 28 DA

In addition, at the precipice between the information provision requirements cluster and the market power balancing requirements cluster outlined below is a grouping of obligations that pertain to transparency and information provision particularly for the purpose of empowering vulnerable parties. This cluster is outlined in the next section.

4.2. Market Power Balancing Requirements

The data economy as it currently stands arguably displays an asymmetry of power both between service providers and service recipients but also between different businesses themselves. While we do not consider the Digital Markets Act in this paper, a legislative instrument aimed squarely at ensuring competitiveness between actors in the data economy, there are other provisions within our scope that have similar purposes.

First are transparency, disclose and general information-related obligations that directly serve to allow individual service recipients to make valid decisions about data pertaining to them and their activities by equipping them with sufficient information.[27] For example, businesses tend to be required to communicate their obligations and the rights of their counterparts as well as the type of data processing operations proactively. European legislation has moved towards minimum standards when it comes to written notices, as exemplified by the privacy notices[28] introduced by the GDPR.

Table 5 – Transparency, Disclosure and General Information Requirements

Data Controller	DISP	DPSP	PIMS	Data Holder	Seller	Hosting Provider	Online Platform Provider
Art. 12–22, 34 GDPR	Art. 12 lit k, h DGA	Art. 24 DA	Art. 15 DSA	Art. 9 para 4 DA	Art. 3 para 2 DA	Art. 16 DSA	Art. 24–27, 39 DSA

Second, and on the basis of the substantive requirements to establish information parity, data-related legislation relies heavily on the concept of consent. One of the main objectives of the European Data Laws is to empower individuals to decide how and where their data is used. In many cases, the laws foresee an individual to give consent to validate the collection and processing of data. As a result, companies are faced with the challenges of consent management. This includes creating and maintaining an infrastructure in which consent can be queried, stored and demonstrated in case of a dispute or questions, but also to ensure that this infrastructure fulfils certain qualitative requirements. As the European legislator is increasingly explicit in its protection of validity of consent,[29] businesses are under similarly increasing pressure to vet their consent management processes accordingly.

Table 6 – Consent Management and User Empowerment Requirements

Data Controller	DISP	Data Holder	Online Platform Provider	Third Party
Art. 6 para 1 lit a, Art. 7 para 1, 3, Art. 21 GDPR	Art. 12 lit n, h DGA	Art. 4 para 6 DA	Art. 25 DSA	Art. 6 para 2 DA

[26] See also Rec 68 GDPR.

[27] These obligations overlap with the public reporting and consultation requirements outlined in Table 1.

[28] See e.g. Art. 30 GDPR.

[29] M. Gartner, 'Regulatory Acknowledgment of Individual Autonomy in European Digital Legislation: From Meta-Principle to Explicit Protection in the Data Act', *European Data Protection Law Review*, 8.4 (2022), 462–73 https://doi.org/10.21552/edpl/2022/4/6.

Third, European legislation also considers market power imbalances between businesses themselves and imposes minimum standards for the contractual relationships between such actors. Companies can generally shape their relationships with customers and other commercial actors as part of their contractual and economic autonomy. However, the present and forthcoming European data-specific legislation lays out certain standards these relationships have to meet from a contractual standpoint.

Table 7 – Contractual Standards Requirements

Data Controller / Data Processor	DPSP	PIMS	Data Holder
Art. 28 para 3 GDPR	Art. 24 DA	Art. 14 DSA	Art. 4 para 6, Art. 8,9,13 DA

European legislation imposes restrictions to ensure fair competition. As a result, companies must monitor their contracting behaviour and ensure compliance with these standards that tend to rotate around fair transparent and non-discriminatory access to services or the underlying data.[30]

Table 8 – Fair Competition Requirements

Data Holder	DISP	*[any] Enterprise*
Art. 9 para 3, 14 para 2,3 DA	Art. 12 (part. lit f) DGA	Article 14 para 2,3 DA

Finally, some legislative provisions oblige businesses to take particular fairness standards into account that require them to actively balance their interests with the interest of their counterparts or even act in their best interest.

Table 9 – Fairness and Equity Requirements

DISP	PIMS	Data Controller / Data Processor
Art. 12 lit m DGA	Art. 14 para 4 DSA	Art. 5 para 1 lit a GDPR

4.3. Governance Requirements

We group obligations that require directional intent towards internal strategic decision-making into a cluster we denote governance requirements. The aforementioned consent management requirements can be considered as lying between market power and governance requirements. However, there are other imposed obstacles to businesses in this cluster as well.

First and foremost, an essential tenet of data-related legislation is its limitation in certain cases. Data has increasingly become a valuable resource for many companies. Nonetheless, the European legislators remain sceptical towards excessive data collection and processing, in particular when this is not connected with the initially conceived purpose of the data operation. Companies face the challenges of justifying their data intake and subsequent operations vis-à-vis the general principle of data limitation / minimization. In addition certain data may be used for some purposes but not others, meaning that companies have to monitor data usage for purpose.

Table 10 – Data Usage and Limitation Requirements

Data Controller	Data Processor	DISP	Data Holder	Third Party	Data Recipient	Provider of very large Online Platforms / Online Search Engines
Art. 5 para 1 lit c, Art. 25 GDPR	Art. 9 GDPR	Art. 12 DGA	Art. 4 para 2, Art. 5 para 5 DA	Art. 6 para 1 DA	Art. 11 para 2,3 DA	Art. 35 DSA

[30] Note that the Digital Markets Act falls out of our scope of inquiry, but that it also serves similar purposes as the provisions identified in this section.

Second, most of the obstacles identified in this paper come with administrative overhead that may often require additional human resources to manage. In certain cases, European legislation actually imposes the need for certain positions to be established and held by qualified personnel, further compromising the organisational autonomy of companies.

Table 11 – Representational and Staffing Requirements

Data Controller	Data Controller / Data Processor	DISP	PIMS	Provider of very large Online Platforms / Online Search Engines
Art. 37 GDPR	Art. 27 GDPR	Art. 11 para 3 DGA	Art. 11–13 DSA	Art. 41 DSA

4.4. Infrastructure and Capacity Requirements

European data-related legislation imposes particular technical processes or outcomes that businesses must adhere to. We first consider issues of security and risk. Strongly connected to the principles that companies ought to ensure integrity and confidentiality of their data are the requirements to create robust and resilient infrastructure and workflow processes to ensure the security of said data. Hardening data infrastructure encompasses adaptation of physical environments, training of staff and development of internal processes, all of which can require significant investment. Companies face fines and reputation damage in case these requirements are not met. We note that this development is still ongoing; for example, shortly before submission of this article, the European Commission has introduced the Cyber Resilience Act, which creates obligations for product manufacturers to ensure their security throughout their lifecycle.[31]

Table 12 – Security and Risk Mitigation Requirements

Data Controller	Data Controller/ Data Processor	DISP	Product Manufacturer / Related Service Supplier	Provider of very large Online Platforms / Online Search Engines
Art. 35 GDPR	Art. 32 GDPR	Art. 12 lit g, j DGA	Art. 3 DA	Art. 34, 35 DSA

Second, we turn to matters of confidentiality. Apart from the general regulations that limit or forbid disclosing or transferring of information, companies must often also adhere to an additional layer of confidentiality, and as a result must take measures to ensure that this confidentiality is guaranteed. In recent legislation, this has been particularly towards the goal of ensuring commercial competition, e.g. with respect to trade secrets. As such, this is closely connected to the Security Requirements outlined above.

Table 13 – Confidentiality and Secrecy Requirements[32]

Data Controller	Data Holder
Art. 5 lit f GDPR	Art. 4 para 3 DA

Finally, serving partly as one of the exceptions to the obligations imposed on companies to limit data storage and derivative information as outlined before are certain archival practices that are required by the European legislator. In these cases, companies must develop processes and capabilities to properly store certain information and have it accessible to certain entities.

[31] See the Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020.

[32] Note that the DGA also contains provisions with respect to confidentiality, but that in that case burden falls on the public entity reusing the data.

Table 14 – Documentation and Archiving Requirements

Data Controller	DISP	Online Platform Provider	*Vendor utilising Smart Contracts*
Art. 30 GDPR	Art. 12 lit o, h DGA	Art. 34 para 3 DSA	Art. 30 para 1 lit c DA

5. Regulation as Commercial Obstacle

On the basis of the above analysis of the European data legislation, we suggest that these fourteen sets of requirements impose five major obstacles for businesses[33] as they navigate the data economy.

First most of these requirements mandate some form of capacity building for businesses; forcing them to create internal personal and infrastructural knowledge and resources to ensure compliant workflows, increasing costs and need for sufficiently trained personnel.[34]

Second, we predict an increased reliance on outsourced solutions. As particularly small businesses cannot develop their tools and workflows to ensure compliance themselves, turning to third-party providers may be a (costly, but still economically sound) consequence. Reliant businesses tend to be in a weaker position that the outsourced service provider, incur additional costs and cede control and understanding of their data-related processes.[35]

A third issue of concern that may affect businesses' competitiveness and efficiency is the adversarial exercise of rights. As the legislation outlined above aims to create parity between different data economy participants, it equips a large number of actors with powerful tools to engage with other businesses. However, some of these can arguably be weaponized; for example repeated subject access requests can create substantial additional work for smaller businesses that have not yet fully automatized their information request workflows.[36]

Fourth, in aggregate, and in close connection to the previously outlined obstacles, compliance with these legislative instruments creates a general administrative overhead. The creation of specific positions requires additional efforts of human relation- and legal professionals, just as data management (e.g. archiving, ensuring access, etc.) requires a certain hardware and software infrastructure. While outsourcing is possible (and an obstacle in itself), managing these requirements still increases the administrative strain on businesses which are ultimately responsible for their compliance.

---

[33] Nb. that many of these obstacles will also affect non-commercial entities as well. Already analysis of some of the instruments referenced above has suggested that there is substantial risk for overhead and loss of efficiency, as well as general uncertainty as a result of the European legislation in the digital domain, see e.g. European Commission, Directorate-General for Research and Innovation and M. Eechoud, *Study on the Open Data Directive, Data Governance and Data Act and Their Possible Impact on Research* (Publications Office of the European Union, 2022) https://doi.org/doi/10.2777/71619. We welcome more research into this area as well, albeit a closer analysis of this is decidedly outside of the scope of this paper.

[34] This comes at a time in which many of the required capacity building resources are already scarce, e.g. at the time of writing there is wide acknowledgment of a global He Li, Lu Yu and Wu He, 'The Impact of GDPR on Global Technology Development', *Journal of Global Information Technology Management*, 22.1 (2019), 1–6 https://doi.org/10.1080/1097198X.2019.1569186.shortage of cybersecurity professionals.

[35] The challenges of such outsourcing is well recognized, see e.g. Daniel Bachlechner, Stefan Thalmann and Ronald Maier, 'Security and Compliance Challenges in Complex IT Outsourcing Arrangements: A Multi-Stakeholder Perspective', *Computers & Security*, 40 (2014), 38–59 https://doi.org/10.1016/j.cose.2013.11.002. See also Subas Roy, Heaney Michael and Hanjo Seibert, *RegTech on the Rise: Transforming Compliance into Competitive Advantage*, 2018 https://www.oliverwyman.com/content/dam/oliver-wyman/v2/publications/2018/may/RegTech-on-the-Rise.pdf for an intra industry perspective.

[36] Mariano Di Martino and others, 'Personal Information Leakage by Abusing the GDPR's Right of Access'', in *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, 2019, pp. 371–85; Tobias Urban and others, 'A Study on Subject Data Access in Online Advertising After the GDPR', 2019, pp. 61–79 https://doi.org/10.1007/978-3-030-31500-9_5; Matteo Cagnazzo, Thorsten Holz and Norbert Pohlmann, 'GDPiRated--Stealing Personal Information on-and Offline', in *European Symposium on Research in Computer Security*, 2019, pp. 367–86.

Fifth and finally, we acknowledge that the comparatively advanced and strict regulative environment may disadvantage data-driven businesses in a global competitive landscape. The aggressive posture on data limitation certainly has the potential to limit the development of innovative products and services in the data economy.[37]

In some contrast to these propositions, the European stakeholders aim to "become the most competitive and dynamic knowledge-based economy in the world"[38] and to become "a leader in a data-driven society".[39] Currently, this "European way" seems rather one-sided with the imposition of additional requirements on actors within the digital domain. The European approach, under consequential weighing of fundamental rights, appears to have perceived the digital domain first as a legal vacuum of sorts,[40] calling for European stakeholders to lead the way in its regulation. But at the same time, businesses are also the intended beneficiaries of this regulatory activity. Balancing-of-interest tests occur in many of the highlighted legal instruments, market power-balancing and data portability rules protect commercial actors, and the imposition of cybersecurity standards is ultimately in favour of the data driven business. Nonetheless, it will be interesting to see how the European legislator will balance the commercial obstacles we identified here with explicit advantages it can provide to offset the cost of compliance. For example, the DGA provides a legal framework for businesses to access information held by public bodies. Similarly, initiatives like the European Alliance for Industrial Data, Edge and Cloud, infrastructure projects like Gaia-X,[41] certification schemes like the European cybersecurity certification scheme for cloud services,[42] codes of conducts or guidance such as the SWIPO data portability code of conduct or the CSPCERT recommendations,[43] and the intended mapping of European data flows all promise to provide a more predictable and fertile environment for commercial activities in the digital domain. At this point, it is too early to say, if this trade-off between substantial compliance requirements for businesses and proactive harmonization of the environment they engage in ultimately favors consumers or commercial actors.

6. Conclusion

In this paper we have analysed four major European legislative instruments and identified 14 shared sets of obligations that impose obstacles on businesses, which we have grouped in four main clusters. We suggest that these regulations can be grouped into clusters of requirements pertaining to information provision, capacity and infrastructure management, governance, and market power and balancing efforts. We have shown that each cluster consists of subsets of obligations and provisions that are in teleological congruence between the different legislative instruments.

Within this context, we have offered a conjecture about the main resulting obstacles for businesses participating in the data economy. Here we have identified issues of capacity building, third-party reliance, adversarial exercise of rights, administrative overhead, and competitiveness as prominent points of concern. Future re-

37 While upcoming legislations' impact is hard to determine there are first insights in how the GDPR has affected competitiveness., see e.g. Michal S. Gal and Oshrit Aviv, 'The Competitive Effects of the GDPR', *Journal of Competition Law & Economics*, 16.3 (2020), 349–91 https://doi.org/10.1093/joclec/nhaa012. However, governance of data-related activities is generally emerging outside of the European Union as well fueled by similar motivations, see e.g. Marina Micheli and others, 'Emerging Models of Data Governance in the Age of Datafication', *Big Data & Society*, 7.2 (2020), 205395172094808 https://doi.org/10.1177/2053951720948087.

38 European Council, Presidency Conclusions, 2000 https://www.europarl.europa.eu/summits/lis1_en.htm.

39 See e.g. the communication material at https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en#:~:text=The%20European%20data%20strategy%20aims,businesses%2C%20researchers%20and%20public%20administrations.

40 See e.g. Dirk Michael Barton, 'Das Internet, Ein Rechtsfreier Raum?', in *Economic Aspects of Digital Information Technologies* (Wiesbaden: Deutscher Universitätsverlag, 1999), pp. 205–25 https://doi.org/10.1007/978-3-322-85190-1_11.

41 For more information see https://gaia-x.eu/.

42 See the communication material re. the EU Cloud Certification Scheme at https://ec.europa.eu/newsroom/cipr/items/713799/en.

43 For more information see https://swipo.eu/.

search verifying and exploring the connection between these clusters and the resulting obstacles for businesses would be most welcome.

Finally we have highlighted that these compliance requirements are part of an implicit trade-off, in which European stakeholders require businesses to accede to high standards but promise to shape the commercial environment in which they engage in towards a healthy and competitive market. Time will tell, whom this trade-off ultimately favors.

Acknowledgement

This paper is part of the LAST-JD RioE project that has funding from the European Union's Horizon 2020 research and innovation programme under the Marie Sklodowska-Curie ITN EJD "Law, Science and Technology Rights of Internet of Everything" grant agreement No 814177. This work was also supported by BitNomos S.r.l.