UiO : Det juridiske fakultet

Obligation to make data available based on exceptional need in the Data Act

Candidate number: 638

Deadline: 25th of November

Number of words: 15436

Table of contents

1 Introduction

1.1 Background and topic

One of the most central privileges of running the State is the right to demand mundane information for the purpose of taxation, including place of residence and other information which is essential for the public bureaucracy. The transfer of data is usually slightly different from the transfer of regular information citizens provide to the public sector. When requesting data, it is often because a public sector body wants data for an extraordinary purpose. When an extraordinary situation arrives, States may request non-personal private data to deal with the crisis. An example is from the recent covid pandemic, where States requested mobile data to monitor the movement of citizens.[1]

Today data is often stored digitally by businesses, frequently in cloud servers,[2] which in of itself makes little difference when deciding when the public sector should have access to private data. It does, however, make a difference for how easily we can store vast quantities of data. Furthermore, with new ways of collecting data, such as by having items digitally transferring data about their own use to databases, the amount of data produced has also massively increased. These factors increase the potential of using data to optimise both public and private activities.

The increasing importance and value of digital data is central the European Union's (EU) economic development. The EU data policy includes making data more freely available for use for both private and public entities across the Union. On the legal front the European Commission is working on several legislations to increase the flow and use of data. One of the proposed legal instruments is the Data Act.

Proposed by the European Commission on 23 February 2022, the Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act) is one of the newer documents in the European set of data legislation. The Data Act is

[1] Iacus et al. (2021), p. 2.

[2] Namasudra (2018), p. 117.

meant to provide the Member State's a basic, common set of rules for several forms of data transfer. It is also meant to increase the total economic benefit in the Union as a "non-rival good" by ensuring desirable rules for "access and usage rights".[3] Chapter V of the Data Act regulates the transfer of data from private entities to public sector bodies when there is an exceptional need for data.

1.2 Research questions

There is no single, obvious answer to how one should understand and evaluate the public authorities' demand for data held by businesses. Legally, there are numerous approaches which have in common that they are based on a form of balance, that the State measure shall be within reason. While some rights are absolute, an intrusion on the right to property can be interfered with if deemed necessary for public or other forms of interest. The topic is addressed in several EU legislations, from the European Charter of Fundamental Rights and European Convention on Human Rights to the data-focused legislation written in this or the last decade.[4] With the potential passing of the Data Act proposal the right to certain forms of property will receive new parameters.

With the potential for great net benefit from data transfer, the resistance from most stakeholders and the question of a new means for the public sector to exercise power in the air, the issue of obligatory transfer should be enlightened.

I raise two research questions in this paper:

1. What are the legal implications of the business obligation to transfer data in Chapter V of the Data Act?

2. Is the business obligation to transfer data to a public sector body when the body proclaims an exceptional need for the private data an acceptable burden to affected businesses?

[3] Commission (2022): Data Act, recital 6.

[4] See Section 4.4

1.3 Methodology

The methodology used to motivate the thesis of the research questions of this paper consist mainly of legal doctrinal methodology, and to some extent law and economics. Naturally, my understanding of European legislation and proposals is based on European principles for legal interpretation. The Data Act proposal is a regulation, which means the legal text will be directly enforced in Member States without being altered in national law. Currently, the Data Act is still a proposal. The trialogue meeting between the Commission, Parliament and Council has not begun. The Act's proposal status means that the document may never be a legally binding legislation. But that the Data Act will be accepted, in its current form or with modifications is likely. The Data Act does regulate certain aspects of data transfer which no other European legislation addresses, and which has been found useful to legally regulate by the Union.

The European Court of Justice (CJEU) is the decisive interpreter of European legislation (cf. the Treaty of the European Union Article 19). There are terms and conditions in the Data Act which are similar or identical to terms described in other European legislation that has been passed or proposed. The CJEU can help with interpreting the more nebulous articles of the Data Act, by having clarified similar terms in active legislation. Furthermore, the CJEU has judged in cases regarding questions of the necessity of public intervention in democratic societies.

Teleological interpretation sets articles in the context of the objectives of a legislation. Context and objectives are important for determining the meaning of articles (cf. Case C-306/12 *Spedition Welter* para. 17). I will use teleological interpretation on the more central articles in Chapter V of the Data Act.

To assist in my interpretation of the relevant legislations and proposals, I will reference and use legal research and documents accompanying the legislations. I reference policy documents and research articles, as many books there thoroughly analysing the European legislation which has recently come into force, or which remains proposals, have not yet been written. I rely on the explanatory memorandum and the recitals to the Data Act to clarify the meaning in the articles and to better determine the purpose and scope of the Act. The CJEU has used explanatory memorandums to reconstruct the intended meaning of articles in

legislations (cf. Case C-108/09 *Ker Optika* para. 25 and Case C-454/18 *Baltic Cable* para. 18). As the preface is not legally binding, the meaning of the articles cannot be reconstructed in such a way that it becomes contrary to the wording in the articles (cf. Case C-136/04 Deutsches Milch-Kontor GmbH v Hauptzollamt Hamburg-Jonas para. 32).

I also use the Impact Assessment Report accompanying the Data Act. The Impact Assessment Report is a preparatory document which lays out the researched and likely effects of the Data Act proposal. It provides insights into the factual background and desired outcome of the Act. Three alternative sets of measures are laid out in the Impact Assessment Report, whereas the second policy option was decided as the preferred option by the Commission's staff.[5] This alternative is therefore crucial for determining how the Commission has predicted the effects of the Data Act proposal. Preparatory work and the preambles of legislation can be used in European law to clarify and elaborate the meaning of articles.

Judicial literature has little to no formal standing as a legal source, but the judicial authors' processing of the law is used by the European Union.[6]

The rest of this paper consist of chapters that address the importance of data in our time and the European reasoning for regulating data transfer in the Data Act, the interpretation of said Act, remarks on the economic effects of Chapter V of the Data Act and lastly a conclusion to the research questions.

2 Introduction to the Data Act: objectives and importance

The Data Act ambitiously lists many objectives. The Data Act is intended to provide European businesses a competitive advantage, as well as help the public sector by substantially increasing the flow of "non-personal data".[7] The main goal of the Act goal is to secure and increase the transfer of data between sectors and between businesses. It shall provide "harmonised rules" for three aspects of data (cf. Article 1(1)). It shall "increase "business-to-business" data sharing, clarify ownership of "co-generated industrial data" and foster business to

[5] Commission (2022): Executive Summary of the Impact Assessment Report, p. 2.
[6] Arnesen, Kolstad, Rognstad and Sejersted (2014), p. 56.
[7] Commission (2022): Data Act, explanatory memorandum, p. 4.

government data sharing". First, it has rules for "data holders" making data available for "data users". Second, it lays down rules on the use of data created by a product or related service for the user of the product. This is probably the most significant of the objectives in terms of impact.

Third, it has rules for making data available by "data holders" to public institutions when there is an "exceptional need" for the data to carry out a task of "public interest". This paper is focused on the third objective. Business-to-government data sharing is handled in Chapter V of the Data Act, which may be the most controversial part of the Act due to the authoritarian nature of obligations and a lack of trust amongst businesses towards the public sector.[8] Hypothetically, it can therefore quickly become the most criticised part of the Act and demands adequate attention. This paper focuses on Chapter V of the Data Act and its impact on businesses, including those that receive the demand for a data transfer, and business in general. The business-to-government data sharing is encouraged in the European data srategy[9] because it will help the public sector to create statistics and to "improve evidence-based policymaking",[10] with the evidence of course being the data and information created by private businesses.

More objectives can be identified in the Data Act's preamble and supporting papers. While the Data Act is meant to increase transfer of data from data holders to the public sector, it should hopefully maintain innovation from private businesses while also increasing data sharing with the public sector.[11] The Union must balance the desire to maintain data generation and "innovation"[12] by businesses against increased data utility for public sector bodies. The overall objective of the Data Act in relation to the data strategy is to increase data sharing by the creation of "cross-sectoral governance framework for data access" and legislating relations "between data economy actors".[13]

[8] Commission (2022): Impact Assessment Report, p. 19.
[9] See Section 3
[10] Ibid., p. 12.
[11] Ibid., p. 26.
[12]Ibid., p. 26.
[13] Commission (2022): Data Act, explanatory memorandum, p. 1.

The Data Act's impression of having a broad scope is reinforced by involving virtually every major group of actors involved with data, including the Union's own "institutions, agencies or bodies" (cf. Article1(2)).

It has been estimated that if data sharing from business-to-government in exceptional situations increases the creation of official statistics by 20 % then it could add between 4.4 and 12.5 billion Euro annually. Furthermore, the streamlined manner in which data is transferred in accordance with Chapter V of the Data Act could even help businesses save 155 million Euro annually.[14] Yet when asked for feedback on the proposal of obligatory data transfer, it was found that most business stakeholders prefer to keep their current freedom to dispose of data, as "voluntary mechanisms are sufficient" and obligations will "unnecessarily increase their costs".[15] It is impossible to know who is right before the Data Act is implemented. For the moment, however, we can look at the aspects of the Data Act proposal to make evaluations about whether the costs to businesses will increase or reduce, and what the benefits for the public sector and the businesses may be.

3 European data strategy and legislation

3.1 The digital single market

Data is one of the most valuable assets of our time. The period in which we live has been named the Information Age,[16] in part referencing the quantity of data, how easy it is to store and access and the buying and selling of it using digital networks and databases. Information has always been of value, but today data is sold on a grand commercial scale; some of the largest companies in our time sell data as the main source of income for the company.[17] The increased quantity of data, its potential utility and its economic importance has not gone unnoticed by the European Union, which now seeks to make a net of legislations which will significantly affect businesses.

[14] Commission (2022): Impact Assessment Report Accompanying the Data Act, p. 49.
[15] Ibid., p. 48.
[16] Bassett, Marris and Thornham (2009), p. 153.
[17] Dutch-Brown and Martenes (2020): p. 7.

The core function of the European Union is to realise the internal market across the Union, as stated in the Consolidated Version of the Treaty on the Functioning of the European Union Article 26(1). While the Union has largely realised an internal market for more traditional industries, there were, and to some extents still are, national laws in Europe which substantially differ in how they regulate data. This has caused frustration as it has been a barrier to trade for those who are involved in the European data economy and must deal with multiple different laws at once across borders. For example, almost half of companies deemed "copyright restrictions" as preventing them from "selling abroad".[18] Other issues are prevalent as well: many businesses have difficulties with acquiring needed data from other companies,[19] and only 8% of companies in Europe can meaningfully capture "value from data".[20]

A common, European set of regulations can help to not only mend the issues facing businesses, but also be an economic boon for the Union. Some of the potential benefits of the European digital initiative include better access to goods and services by breaking down barriers for "cross-border online activity"[21], and a common digital market would allow consumers to save up to "EUR 11.7 billion"[22] yearly and can increase the availability of capital and ease the access to several elements of the digital economy, such as "cloud computer infrastructures".[23]

Union legislation has so far shown to be crucial in understanding the direction of data regulation on a global scale. There are several reasons for this. The European regulations have a substantial legal effect on Member States and members of the European Economic Area. Furthermore, because states outside of the Union must comply its legislation to sell goods and services in the Union area, the EU is essentially pursuing a "global order".[24] European data legislation will be relevant on a near global scale and is of prime value for study. In the Commission's own words, the EU will remain open to those who will "play by European rules".[25] One of the greatest motivations for the Union's work with data legislation is to utilise the increasing economic value of data, which is estimated to yield as much as "14 % of cumulative

[18] Commission (2015): A Digital Single Market Strategy for Europe, p. 7.
[19] Commission (2022): Impact Assessment Report, p. 8.
[20] Ibid., p. 8.
[21] Ibid., p. 3.
[22] Ibid., p. 3.
[23] Commission (2014): Towards a thriving data-driven economy, p. 4 and 6.
[24] Bradford (2020), p. 24.
[25] Commission (2020): Shaping Europe's Digital Future, p. 2.

additional GDP"[26] by 2030. A part of this is the increased utilisation of private data by the public sector.

The plan for streamlining European activity and legislation relating to data and general digital activity began last decade. Some issues related to data have been deemed unresolved,[27] and many of the affected parties have voiced a wish for more supplementary legislation. This has been an important motivation for the Union to plan out a more controlling and far-reaching strategy which shall be executed this decade.

3.2 The European Data Strategy

3.2.1 General goals

One of the most important areas of prioritisation in the European data policy thus far been strong protection of personal data. Such data protection is a protection of the fundamental right to privacy on the digital front.[28] The Union has also passed several legislations strengthening data confidentiality and integrity.[29] Meanwhile, the Union additionally wishes to increase the sharing and use of digital data, the Commission has proposed legislation that will increase the availability of data, even when the goal is not purely or even partly commercial, but instead to support public sector bodies with private information, or vice versa.

The Commission has a "vision" of Europe in 2030 where "almost infinite" quantities of data are easily available for businesses and other parties, but also were "sensitive business data" is secure.[30] Businesses are to be provided a "framework" that lets them "pool and use data" and to compete on "fair terms".[31] The Union wants to challenge the "Big tech" companies which each control significant portions of digital data, most of whom are based in the United States. Europe will build a "data-agile" economy that balances "the flow of data".[32] The

[26] Ibid., p. 4.
[27] Commission (2022): Impact Assessment Report, p. 3 and 4
[28] Commission (2016): General Data Protection Regulation, recital 1.
[29] Commission (2020): The European Data Strategy, p. 4.
[30] Ibid., p. 4.
[31] Commission (2020): Shaping Europe's digital future, p. 1.
[32] Commission (2020): A European Strategy for Data, p. 3.

Commission's vision with the digital single market is to help make Europe a "leader in data economy" to benefit its economy and society.[33] In short, the Union wants to prop up both the European share of data-related commerce and increase the ease of use of data.

To realise the vision, Union has several, broadly encompassing goals and measures. They include that all data driven-products and services comply with "norms of the EU single market", rules of access to data are "fair, practical and clear", securing that "data-fuelled" products and services can "depend on the highest cybersecurity standards", increase sharing of data public-to-private, amongst businesses and from businesses to governments, improved data infrastructure by better use of their "cloud-service" and common "data spaces" for many fields.[34]

3.2.2 Legislation in the Data Strategy

Directive 2019/1024 (the Open Data Directive) is meant to help parties reuse data in the form of documents and research data held by the public sector bodies (cf. Article 1). One of the directive's goals is to prevent public sector bodies from charging more than a marginal cost for data reuse and should generally be "free of charge" (cf. Article 6). The directive is meant to increase efficient use of data held by the public sector. It increases the transfer of data government-to-business. Like the Data Act, the Open Data Directive is meant to increase use of data by compulsory means. The Data Governance Act proposal is one of the major proposed legislations in the European Data Strategy. Like the Open Data Directive, it too is meant to increase the sharing of "certain categories" of public data (cf. Article 1(a)). It is also meant provide a framework for altruistic data sharing (cf. Article 1(c)). The Data Governance Act shall also be a legal basis for a "supervisory" framework for the provision of data sharing services (cf. Article 1(b)).

Regulation 2016/679 (the General Data Protection Regulation (GDPR)) is a thorough protectionary legislation for personal data. The rest of the data strategy should be understood in the context of the GDPR, as other legislations primarily regulate the sharing of non-personal data. If personal data is shared, it will be with considerations to the protection the GDPR provides.

[33] Ibid., p. 1.

[34] Ibid., p. 5, 7, 8 11 and 13.

Regulation 2018/1807 (the Free-flow Regulation) aims at increasing the sharing of processed electronic data within the Union (cf. the regulation's Article 1). It tackles aspects of data sharing between professionals, such as information requirements for port data (cf. Article 6.)

A directive which defines a frequently used term in the Data Act is Directive 96/9/EC (the Database Directive), which is mentioned in the Act's preambles.[35] A database is regarded as a collection of data "arranged in a systematic or methodical way" and "individually accessible" electronically and includes protection of "certain rights" relating to intellectual property (cf. the Database Directive Article 1(2) and Article 2(b)) respectively. However, the Data Act "clarifies" the protection of databases in the Database Directive, by dismissing data created "as a by-product" of economic activity which is not directly an investment in the database.[36] This is especially relevant for data produced by devices which uploads data about their use to the Internet of Things.

Several of the regulations mentioned are relevant for providing context to the Data Act, for interpreting certain terms or to either stipulate limits on the reach of the articles or to specify their implications. Some of them are directly mentioned in the preface to the Act or in the articles themselves. For example, the Act shall be "consistent with existing rules on processing personal data", with a reference to the GDPR. [37] The Act shall not be interpreted in such a manner as to "limit" the right to protection of personal data.[38] This means that the full understanding of the GDPR is applicable to the Data Act. Transfer of data which can be identifiable, must uphold the standards of the GDPR.[39] The relevance of other legislation will be made apparent in Section 4.

There is more relevant legislation in the data strategy, but those presented here are among the most central. The combination of legislation in force and new proposals covers several aspects of data transfer and security. Unfortunately, the current framework for data sharing business-to-government makes it difficult to acquire data on an ad-hoc basis.[40] Chapter V of the

[35] Commission (2022): Data Act, recital 64.
[36] Ibid., explanatory memorandum p. 9.
[37] Commission (2022): Data Act, explanatory memorandum p. 3.
[38] Ibid., recital 7.
[39] Ibid., explanatory memorandum p. 3.
[40] Commission (2022): Impact Assessment Report, p. 19.

Data Act is meant to adjust this by making business-to-government data transfer compulsory when the public sector has an exceptional need for private data.

Like the Data Governance Act proposal, the Data Act is a direct link in the European data strategy. It was deemed a necessary part of the strategy because it regulates aspects of data sharing and data ownership that is not adequately covered in other legislations. It lays down ownership of co-generated industrial data. Such data is a by-product of the use of products, when there are multiple parties involved in the data generation.

4 Chapter V of the Data Act: Making data available to public sector bodies and institutions, agencies or bodies based on exceptional need

Chapter V has a legal basis for public sector bodies and union institutions, agencies, or bodies to request a data transfer based on exceptional need. The framework for data transfer should be "harmonised",[41] which we can understand as a requirement for reasonableness. Chapter V is central for understanding the obligation to transfer data based on request, as its title suggests, and the central chapter for answering this paper's research questions.

This chapter is an analysis of the Data Act's most crucial legal text for understanding the duties businesses will have with regards to data transfer to public sector bodies. It is desirable to have an exact understanding of when and how a public sector body can demand an obligatory data transfer. This is paramount for a better conclusion to the question of whether the obligation to transfer under such conditions as when there is an exceptional need is justified.

4.1 Article 14: Obligation do make data available based on exceptional need

The actual legal basis for a public sector body to request a transfer of data is in Article 14 of the Data Act.

[41] Commission (2022): Data Act, explanatory memorandum p. 15.

Article 14 states: “Obligation to make data available based on exceptional need

> 1. Upon request, a data holder shall make data available to a public sector body or to a Union institution, agency or body demonstrating an exceptional need to use the data requested.
> 2. This Chapter shall not apply to small and micro enterprises as defined in Article 2 of the Annex to Recommendation 2003/361/EC.”

Article 14 implies a possibility for public sector bodies to legally demand data upon request from private businesses, when there is an “exceptional need”. There are several terms in the article which require interpretation.

4.1.1 Parties in Chapter V

Public sector body refers to any organisation that acts as a public authority or which delivers a public service. They include “national, regional or local” authorities and organisations ruled by “public law” of the “Member States” (cf. Data Act Article 2(9)). A public sector body is understood separately from a normal data receiver in the Act, as a public sector body does not fulfil the condition of acting for a “trade, business, craft or profession” (cf. Article 2(7)). Companies that are mainly publicly owned fall outside the scope of this paper, as they are neither formally established as a public body nor will they have the authority to request a data transfer as described in Chapter V.

While public sector bodies as a main rule only refers to public authorities, “research-performing” and “research-funding” organisations can be deemed public sector bodies or bodies “governed by public law”.[42] This entails a broader inclusion of organisations and institutions which can demand obligatory data transfer than what a traditional and natural understanding of public sector bodies includes.

Data holder is defined in the Data Act. The relevant parts of the definition are that a data holder is anyone who has an “obligation” to make data available, or in the case of “non-personal data”, the ability to make available “certain data” by “technical design of the product

[42] Ibid., recital 56.

and related services", in accordance with the Data Act, "Union law" or "national legislation" implementing Union law (cf. Article 2(6)). The inclusion of those who can make data available through technical control relevant for businesses as "manufacturers" who can chose to generate or transfer data using products connected to the Internet of Things.[43]

While the definition in Article 2(6) includes both natural and legal persons, the explanatory memorandum makes it clear that Chapter V only involves "business-to-government", and that there can be made a demand for data held by "enterprises".[44] that are not considered micro or small. Hereby, I use business to refer to the data holder described in Chapter V. Micro and small enterprises are defined in Recommendation 2003 361/EC (recommendation for the definition of micro, small and medium-sized enterprises) Article 2(2) and (3); micro and small enterprises employ fewer than 50 persons, alternatively have an annual balance sheet total not "exceeding EUR 10 million". Protecting smaller businesses from requests from public sector bodies is part of the Data Act's goal of ensuring "fair data access".[45] The inclusion of smaller businesses could have made data sharing business-to-government unreasonable, because smaller businesses will sometimes lack the means to comply with requests.

4.1.2 Data

The parties in Chapter V are now presented. We still need to comprehend the object for transfer. Data is defined in the Data Act as any digital "representation" of "acts, facts or information" (cf. Article 2(1)). This is an astoundingly broad definition. Information in this context usually refers to meaningful knowledge of certain acts and/or facts. Data can alternatively be separated into four groups: raw, pre-processed, processed and data-driven insights[46]. Raw data is typically pure facts, such as numbers. Pre-processed data is data which has undergone various forms of selection and transformation. Processed data is data manipulated into "meaningful information".[47] Insights are conclusions drawn from processed data.

[43] Ibid., recitals 19 and 24.

[44] Ibid., explanatory memorandum p. 14 and 15.

[45] Ibid., recital 5.

[46] Commission (2020): Towards a European strategy on business-to-government data sharing for the public interest, p. 23.

[47] Ibid., p. 23.

From the general wording of data in the Data Act, all the mentioned categories of data fall under data which can be demanded to be transferred by a public sector body, if the data is stored digitally. This wide-reaching definition is meant to secure "consistency with the Data Governance Act".[48] The Data Act pays special attention to data produced as a by-product of use by connected devices, but the definition in Article 2(1) makes it clear that data can encompass much more. The data produced as a by-product of use of the connected devices will often be tied to how and how frequently the device is used.

Data in the Data Act also includes "complications" of the mentioned representations of data, such as "recording" (cf. Article 2(1)). Taking into consideration the example used in the article, data can be shared in any medium and still be considered data or information. Data which can be transferred can principally involve any confidential information. This can include intellectual property. However, there are two prominent categories of data property: database protection and trade secrets.[49]

It is stated outright in the Database Directive Article 3(1) that databases are to be regarded as intellectual property, though the majority opinion amongst respondents in a study from 2018 would not include machine-generated data as intellectual property.[50] The property status of databases was presented in Section 3.2.2.

Intellectual property is special in that it does not directly cause any costs for the party which shares it, unlike a transfer of other property such as money or objects. Therefore, the case for the sharing of data is strong. However, it is implied that the intellectual property has costs associated with its acquisition. For example, the research costs for creating a new form of medicine can be substantial source. If someone who does not initially own the medicine can legally demand the formula, the creators of the medicine can suffer competition from others who did not bear the costs associated with the creation of the intellectual property. Once the data has been transferred, it can easily be transferred again, until it is well-known.[51]

[48] Commission (2022): Impact Assessment Report, p. 1.

[49] Graef and Husovec (2022), p. 4.

[50] Commission (2018): Study in support of the evaluation of Directive 96/9/EC on the legal protection of databases, p. 20.

[51] Eide and Stavang (2018), p. 231.

The Data Act regulates the access to data which can fall under what is deemed trade-secrets, with a direct reference to the Directive 2016/943 (Trade Secrets Directive) in the Act's Article 8(6). A trade secret is information that is not "generally known" or "readily accessible" to persons who are in the "circles" that normally "deals with the kind of information in person", which has "commercial value" because of its secrecy and is kept secret due to "reasonable steps under the circumstances" by the person who is "lawfully in control of the information" (cf. the Trade Secrets Directive Article 2(1)). A trade secret holder can be a "legal person" (cf. Article 2(2)), which means that businesses mentioned in the Data Act can be holders of trade secrets.

While public sector bodies should in principle only be demanding data that is non-personal in nature, this does not completely stop public sector bodies from demanding data which can include something identifiable when it's strictly necessary, as alluded to Section 3.2.2 concerning the application of the GDPR. In the context of a request of a request for transfer of non-personal data, and personal data cannot be reasonably separated from the non-personal data, the inclusion of personal data can be "strictly necessary". Then the business should, when possible, anonymise the data. [52] Anonymising personal data means the identifiable information is presented in such a way that persons cannot be identified in it.[53]

The data requested is not publicly available, yet the public sector body showing interest in the data must have some knowledge about the kind of data the business possesses. If we continue with the example of the public sector desiring data on monitoring the movement of citizens, from Section 1.1, the public sector will know that the relevant business had relevant data due to the services of the business. For various legal reasons, it can be expected that the companies would orderly keep the relevant data, at least as long as it was defensible to not delete the data.

The fact that the rights based in the GDPR shall not be infringed upon by the provisions in the Data Act[54] can give context to the understanding of common terms in the Act and the GDPR. This is quite reasonable when only looking at the protection of personal data. One question is

[52] Commission (2022): Data Act, recital 64.
[53] Commission (2016): General Data Protection Regulation, recital 26.
[54] Commission (2022): Data Act, recitals 7 and 8.

whether terms in the Data Act can borrow content from the GDPR beyond situations where personal data is processed due to transfer, where there is mixed data. As mentioned, the Commission has stated its wish for a common understanding for core vocabulary concerning data. Unequal understanding of central terms such as public interest, in different legislation, is undesirable. Setting aside the particular context for public interest in each legislation, a common understanding of the term in both items of legislation is preferable for consistency.

The interpretation in this section shows that specific parts of data, like personal data, are given attention and clarification, but the data term overall is still broad. The Commission has stated that European legislation could benefit from interoperable "specification" of more accurate data terms, in the form of "ontologies", "core vocabulary", etc.[55] Until such terminology is possibly collected in one document, we can utilise the definitions in current legislations for a more precise understanding.

4.1.3 Conditions for transfer in Article 14

Article 14 does not have a direct definition of what constitutes "exceptional need". Instead, exceptional situations which fulfil the criteria of exceptional need in Article 14(1) are presented in Article 15. This fits with the public sector body having to "use" the requested data. Data can't be used in a conventional sense, but it can help a public sector body to better respond to an exceptional situation.

Article 14(2) references the exclusion of small and micro businesses which I explained in Section 4.1.1. Note that the wording in recommendation for the definition of micro, small and medium-sized enterprises in Article 2(1) is the same as the one in its Annex I Article 2(1), which is referenced in Article 14(2). That Chapter V shan't apply to small and micro businesses implies that the obligation for the business to comply is unapplicable for such businesses. Furthermore, interpreted by its wording, other standards for communication in Chapter V does not apply to small or micro business. They would not have to inform the public sector body that the obligation is null towards it if they receive a request. Such a requirement for communication may follow of other legislation.

[55] Commission (2022): Data Act, recital 79.

Chapter V's Articles 14 and 15 are decisive for determining when a public sector body can demand a transfer of data when there is an exceptional need. Together they are the legal basis for a public sector body to request a transfer of data from businesses. The right to demand transfer of data from businesses by a public sector body is stipulated in Article 14, but the essential conditions for such a transfer being legitimate appear in Article 15.

4.2 Article 15: Exceptional need to use data

Article 15 is the article in Chapter V which deserves the most attention. It is long with combinations of quite vague conditions to fulfil for a public sector body to able to demand a data transfer.

Article 15 states: "Exceptional need to use data

> An exceptional need to use data within the meaning of this Chapter shall be deemed to exist in any of the following circumstances:
> (a) where the data requested is necessary to respond to a public emergency;
> (b) where the data request is limited in time and scope and necessary to prevent a public emergency or to assist the recovery from a public emergency;
> (c) where the lack of available data prevents the public sector body or Union institution, agency or body from fulfilling a specific task in the public interest that has been explicitly provided by law; and
> (1) the public sector body or Union institution, agency or body has been unable to obtain such data by alternative means, including by purchasing the data on the market at market rates or by relying on existing obligations to make data available, and the adoption of new legislative measures cannot ensure the timely availability of the data; or
> (2) obtaining the data in line with the procedure laid down in this Chapter would substantively reduce the administrative burden for data holders or other enterprises."

Article 15 contains five exceptional situations which are deemed to place public authorities in a position where there is a need for data that justifies an obligation to a transfer of data. The five situations will in the following subchapters be covered in detail.

4.2.1 Public emergencies

The three situations described in Article 15(a) and (b) revolves around public emergencies that affects the population of a Member State. A data holder is obliged to publicise data if the data is necessary to respond to, or to prevent or recover from a "public emergency" (cf. Article 15(a) and (b) respectively.

For a crisis to be deemed a public emergency in the Data Act, there must be a risk of "serious and lasting" repercussions on "living conditions" or "economic stability, or "substantial" degradation of economic assets in the Union or in Member States (cf. Article 2(10)). The article sets up a common and three alternative conditions for public emergencies.

Lasting repercussions entails that something will last for a long time. Combined with "serious", the risk of damage must be major and enduring. The consequences, however, should be understood as what will likely happen with a lack of an appropriate response. If for example a devastating drought occurs in a Member State, the likely outcome would be serious harm to food production and perhaps even the emptying of water magazines. But the appropriate response can mend the negative effects, perhaps with the help of data from a private company involved in agriculture or drought relief.

Degradation of economic assets and economic stability are clearly tied to economy and would probably be measurable in terms of money. The consideration of assets is a clear measurement of the actual or potential economic loss due to the emergency. Economic stability is not defined in the Data Act. The Union Treaty on Stability, Coordination and Governance can provide concrete numbers on government debt, growth, etc. Although, as this paper is focused on national public sector bodies, it should be noted that national comprehension of what is a significant degradation of economic stability can be determining.

Living conditions reference our quality of life and can be purely economic or have elements that are economic. Regardless, it is the only alternative condition in Article 2(10) which opens for consideration of non-economic facets when evaluating emergencies. As shown in the next paragraph, the examples in the preamble of the Data Act opens for considerations of the loss of life, spread of disease etc.

Examples of public emergencies vary from health emergencies or "major" natural disasters, including those which stems from climate change to man-made disasters, such as cybersecurity-incidents.[56] The examples are not exhaustive but provide indications of the sort and scale of the crises which are deemed public emergencies. While not provided as an example in the Data Act, war will often count as a public emergency, and is used as an example in the European Convention on Human Rights Article 15. In addition, Member States can stand in solidarity if a Member State is the "object of a terrorist attack" or the victim of a disaster, which can allow the Union to mobilise "all the instruments at its disposal" (cf. the Treaty on the Functioning of the European Union Article 222(1)). Disaster is understood as a negative situation which has a "severe impact on people, the environment or property" (cf. Council decision (2014/415/EU) Article 3 nr. 3). Neither war nor the precise understanding of disaster mentioned in the Council decision are covered in the Data Act. One can argue, however, that either, though war especially, can affect the economic situation of the country to such an extent that it would be covered by the understanding of public emergency in the Data Act Article 15.

The examples provided in the Data Act's preamble as well as in the other mentioned European legislations qualitatively specifies what can be expected to be termed as emergencies. The emphasis on emergencies with a medical side aspect is expected, as the desire for private "mobility data" was desired during the Covid-19 outbreak in Europe.[57] An outbreak of at least the same severity could clearly fulfil the criteria of a public emergency.

It may not be clear what a public sector body would do with business data to optimally tackle an emergency. The mobile data which public sector bodies desired during the Covid-19 outbreak mentioned in Section 1.1 could have been used for a better overview of where citizens spent their time. In the case of a serious food shortage, the public sector may want data related to agriculture and company techniques for transporting food.

Quantitatively, public emergencies remain vague in the Act. No concrete numbers are provided for what constitutes a natural emergency or how grave a cyber incident must be in order to be classified as an emergency. Such vague wording does not provide public sector bodies a

[56] Ibid., Recital 57.

[57] ODI, The GovLab, Cuebiq (2021), The use of mobility data for responding to the COVID-19 pandemic, p.11.

"systematic" and expansive opening to use private data[58]. This alone is probably not enough to deem Article 15(a) and (b) as too ambiguous to be a legal source for exercising authority. Nonetheless, a more elaborate explanation of the minimum scale required for something to be deemed an emergency in Article 15 would be welcome. They situations do not have a clear quantitative condition. A factor in the Data Act which may provide reason to except a quantitative condition for public emergencies, are their economic nature. Of course, in times of high inflation a stated sum of money would quickly lose its original meaning. But a percentage of national revenue which is estimated to be, is in danger of or has been lost, in accordance with the different time aspects in Article 15(1)(a) and (b), could be given at least as a base for evaluation. The assistance given for quantitative calculations within Union legislation is found within the Union Treaty on Stability for measuring economic stability if the Treaty will be applied nationally.

It is certain from the choice of using "exceptional" and "emergency" that obligatory data transfer from businesses to a public body sector shall not be regular, but rather sporadic, even more so than with exceptional needs with basis in letter (c). Such and understanding can be viewed as coherent with the wish for reasonable access to private data under. If public sector bodies could demand transfer of data with milder conditions, it could be an excessive burden on the businesses. But when a crisis can, is or has occurred then asking private businesses to bear a part of the responsibility for getting the nation out of the crisis is more easily viewed as reasonable. To provide more concrete numerical conditions for a public emergency will reduce the current flexibility of Article 15(a) and (b).

To demand a transfer of data from private companies in the case of preventing or recovering from an emergency the circumstances must be "reasonably proximate" to the "public emergency in question".[59] Reasonably proximate would for prevention or recovery include an element of time, and for all three alternatives there is a requirement for adequacy. Of the times the request for data can be made by a public sector, for "prevention" of a public emergency is the one which invokes most uncertainty. A requesting institution would have the put forth the most convincing demonstration to request data when it unknown if an emergency will happen.

[58] Tarkowski and Vogelez (2022), p. 1.

[59] Commission (2022): Data Act, Recital 58.

Not all emergencies will be easy to detect, and therefore it can be unintuitive to acquire data to prevent them. One may wonder if a data transfer from a private company can ever be deemed necessary because a cyberattack may soon occur. Yet even in such a situation, one can make a case for the necessity of private data. The rate of cyberattacks have overall increased significantly. But the increase in attacks have not been even across sectors. Sectors such as healthcare and communications are more frequently attacked than transportation.[60] Attacks against the public health services can increase the mortality rate of patients by disrupting hospital operations.[61] Such incidents will likely fulfil the condition of affecting the living condition of the public. If many software applications become useless due to a cyberattack, then one can argue that there have been "serious and lasting" repercussions, and of course one can argue the same if there is a substantial increase in mortality rates at hospitals. A single moderate attack against a hospital is not a public emergency on its own. But a serious attack, with data which predict a significant increase in the attack against public health services may be ground for requesting data from a private cybersecurity company. Likewise, a threat from a hacker to disrupt multiple public health services, or frequent attacks on a neighbour Member Sate country can be grounds for public health administration to request data.

4.2.2 Data transfer due to public interest that has been explicitly provided by law

There will be deemed to be an exceptional need if a "lack of data" hinders the public authority from "fulfilling a specific" task which is in the "public interest" and which has been "explicitly provided by law", and either the public authority cannot obtain the data by other means or if obtaining the data would "substantially" reduce the administrative burden on data holders or other enterprises (cf. Article 15(c)). The condition of a lack of available data can be relevant when for example there is a "timely complication" of official statistics.[62]

Public interest means that something is of common benefit, which is so broad that it means little without proper context. Public interest has been used differently in general as well as in other European legislation. The wording itself is ambiguous and leaves room for

[60] Brooks (2022)
[61] Mensik (2022)
[62] Commission (2022): Data Act, recital 58.

interpretation.[63] The most important factor for narrowing down what the public interest is in the Data Act, is that it must be provided by law. The public interest should be proportional to the required use of data.

The Expert Group on B2G Data Sharing, an expert group appointed by the European Commission to provide recommendation on business-to-government data sharing, gave an understanding of public interest. The overreaching point of data transfer from businesses to the public is to be for the improvement of "general welfare".[64] Based on earlier court judgements regarding "services of general economic interest", which emphasised the context-specific judgement of what is a valid general economic interest, the Expert Group applied a similar standard to public interest.[65] With such an understanding, trying to give a clear general definition of public interest is unnecessary.

From another perspective, one ought to acknowledge the "political essence" which will come to play when claiming something is for the public interest. As the political and legal leaders of different Member States will have diverging notions on what constitutes public interest, we can expect "diverging implementations" if the meaning of public interest is not solidified.[66]

When interpreting Union legislation, its relevant to not only look at context and objectives, stated in the preface. It is also relevant to look at other Union legislations "as a whole" for a broader context (cf. Case C-621/18 *Wightman* para. 47). Such interpretation can be relevant for the Data Act.

In the GDPR Article 6(1)(e), public interest grounded in a legal basis is considered a legitimate basis for processing data. Like the GDPR, where the processor must have a goal for processing data which fits with a legitimate basis, the public sector body in accordance with the Data Act must have a goal for the data transfer which can be deemed to be in the public interest. In addition, the public sector body must fulfil one of the two alternative conditions in the

[63] Öjehag-Pettersson and Padden (2021), p. 494.

[64] Commission (2020): Towards a European strategy on business-to-government data sharing for the public interest, p. 3.

[65] Commission (2020): Towards a European strategy on business-to-government data sharing for the public interest, p. 16 and ases C-179/90 *Merci convenzionali porto di Genova* para. 27, C-242/95 *GT-Link A/S* para. 53 and C-266/96 *Corsica Ferries France SA* para. 45.

[66] Chu (2022), para. 9.

Data Act Article 15(c) nr. 1 and nr. 2. The term can be understood similarly in the Data Act, because of the mentioned similarities.

To enhance our understanding of what public interest constitutes, we can use legal sources and other opinions applied to public interest in the GDPR. As has been written about the public interest described in the GDPR, it would be unreasonable to interpret it as something which has to be beneficial for most of society, though a public interest should be favourable to more than just a specific group.[67] Such an expectation of the scope of the benefit is transferable to the Data Act.

What is probably not transferable are the different levels of public interest indicated in the GDPR, which separates normal public interest in its Article 6(1) (e) and "substantial" public interest in Article 9 letter (g). Although the conditions in the Data Act Article 15(c) nr. 1 and nr. 2, which require the obtaining of data by other means to be legally impossible and to "substantially" reduce "administrative burden" respectively, indicate that the public interest must be significant. Such an understanding would be in line with the point of the obligatory data transfer only being applicable when there is an "exceptional need".

Another data legislation which helps to broaden the public interest is the Open Data Directive. In the directive's recitals, public interest refers to "public security" and "public health and safety".[68] These examples are public services, which can be a fitting understanding of what public interest is in the Data Act. The combined conditions of "provided by law" and "public interest" will often mean that the public sector bodies will provide a public service. This corresponds with the meaning of public interest given in the Public Consultation on the Data Act: "general benefit to society" and "improvements to public service".[69]

4.2.2.1 Data unavailable by other means

An alternative condition for obligatory data transfer in Article 15(c) nr. 1 is that data which the public sector body has been "unable to attain" by means such as purchase "on the market

[67] Schartum (2020), p. 131.
[68] Commission (2020): Reuse of public statistics, recitals 16 and 31.
[69] Commission (2021): Public consultation on the Data Act, p. 9.

at market rates" or by use of "existing obligations", or if legislative measures will not "ensure the timely availability" of the data. Of course, when a business has a monopoly on certain data and is not willing to sell it, the data is usually only legally available through an agreement with the business.

Excluding the convenient suggestion of using existing obligations, the given examples does not set a clear bar for when the unavailable criteria is met. How much above market price must a purchase of the data be, or how certain and how "timely" must a legislation that grants the public sector a right to demand the data be? Like with public emergencies, the quantitative aspect of the alternative measures in Article 15(c) nr. 1 are vague.

Read together with the given examples in the legislation, "unable" cannot be interpreted literally, but little else can be interpreted as for where the threshold lies. Besides the limitations of market price and existing legal obligations, several expected actions can be imagined. Without further clarification, Article 15(c) nr. 1 is one of the most uncertain statuary provisions in Chapter V, due to the vague notion of what unable is.

The notion that a public sector body would need a transfer of private business data to fulfil tasks provided by law is unusual. If a public interest is provided for by law, there is a high probability that it has the nature of a public service. A public service is regularly provided and usually does not need a sporadic transfer of data from certain private businesses.

When is Article 15(c) nr. 1 relevant and applicable? The "specific task" must be something concrete that the public sector body must do in order to fulfil its more general service. For example, a statistics bureau could have a legal obligation to provide statistics on agriculture. Its specific task is to gather data and provide statistics about a robot which detects diseases in crops. The data about the accuracy of the detections are held by the business which produces the robot. The business has been unwilling to sell the data at a reasonable market price, and no national law allows the bureau to demand the data on the robot. In such a situation, Article 15 (c) nr. 1 can be relevant.

There are companies that offers data which is requested by public sector bodies. The companies Telefonica and Deutsche Telekom have worked with public sector bodies by providing data for statistics. Both companies provided data from their respective "mobile phone

network".[70] Their contributions ensured a higher quality, and a more frequent release of the statistics. A question is if it would be justified to use Article 15(c) nr. 1 for such purposes, provided that the data cannot be bought at a market price and there are no guaranteed legislations with obliges the transfer of the requested data. Presuming that the contribution from the private companies have only upped the quality of the service to the statistics bureaus, it is likely that such data falls outside the scope of Article 15(c) nr.1. The provided quality is at best an edge case of what can be considered a "specific task". A generous interpretation of what data is included is probably not intended when looking at the narrowing conditions for application of Article 15(c) nr. 1. Furthermore, a general improvement in quality is not an "exceptional need" (cf. Article 14(1)).

Article 16 of the Data Act contains exceptions from the public sector body's right to request data that is especially relevant for Article 15(c) nr. 1. The right to request data shall not be used by public sector bodies in relation to "criminal or administrative offences or the execution of criminal penalties, or for customs of taxation" (cf. Article 16(2)). Even if it can be in the public interest, and certain businesses hold key data for investigation of crime, Chapter V cannot be used for such a purpose, likely because it would interfere with the rights to privacy for businesses and principles of criminal law.

Paradoxically, Article 15(c) nr. 1 manages to both have a quite narrow field of application, while also having a key condition which is vague. It may be up to a public sector body's ability to acquire data which determines whether it can request transfer of data from a private business.

4.2.2.2 Substantial reduction of administrative burden

An obligatory transfer, which "in line with the procedure" of Chapter V of the Data Act must be a substantial reduction of "administrative burden" for "data holders or other enterprises", is an alternative condition for demanding a transfer of data from a business in the Act's Article 15 (c) nr. 2. Administrative burdens are the resources we spend for interaction with the public sector. In this context they are the compliance costs businesses have due to the public sector's

[70] Godel et al. (2022), p. 25.

demand for data.[71] In accordance with the Act's principle of proportionality, "substantial" should here not only imply that the transfer of data is of some importance, but of such importance that it outweighs the interests of the business who receives the request for transfer of data.

Subparagraph nr. 2 should be read in context with the rest of letter (c), which states that the transfer should be for a "public interest" "provided by law". This manner of obtaining data should be an efficient alternative for fulfilling the legally protected public interest, with the added consequence of reducing administrative burdens for other businesses who also have a form of obligation to transfer data to the public sector.

The transfer of data will cause a reduction of administrative burdens if it can desirably "replace existing reporting obligations".[72] For various reasons, businesses establish a data partnership with the public sector. Several factors can make this time-consuming. Negotiations can drag on. The same kind of public sector bodies may request the data from the business multiple times. A relevant example is from Germany, where 213 cities of similar size each requested data for traffic management and other urban tasks.[73] By following the method in Article 15(c) nr. 2, both the public and the business could save time, especially due to the Once-Only principle in the Data Act. The principle involves businesses only receiving a data request once from a public sector body, which may share the data with other bodies later. With the estimated growth of data partnerships between businesses and governments,[74] Article 15(c) nr. 2 will likely be used frequently.

4.2.3 Reflections on Articles 14 and 15

The public sector body's right to request data transferred from private businesses with potential fines in the case of refusal, is perhaps the sternest measure in the Data Act, with the potential penalties for disobeying the use of State force as stated in Article 33. Analysing the essence of the right to request data transfers and the consequences of such an obligation for businesses, is central for evaluating whether the Union can uphold incentives for data

[71] Commission (2022): Impact Assessment Report, p. 13.
[72] Ibid., p. 34.
[73] Commission (2022): Study to support an Impact Assessment, p. 231.
[74] Ibid., p. 231.

production and innovation while also increasing the utility of data when the State is sorely in need of data.

The principle of proportionality must be followed by the public sector bodies that decides to request data in accordance with Articles 14 and 15. A goal of the Data Act is to not enact measures are not stricter than "necessary to achieve the objectives".[75] As "exceptional" would suggest, the right to demand a data transfer is meant to be on an "ad hoc basis".[76] Acquiring business data will hardly ever by a nuisance for a public sector body and can help them tackle the situation. But all the exceptional situation requires the data to some extent to be necessary for tackling the situation. This is the standard for proportionality in Article 15. The word "necessary" implies that the public sector bodies must have the data to optimally respond to the emergency. But the standard can't be that it would be nearly impossible to tackle the emergency otherwise, as one can always argue that there are other ways of tackling the crisis which does not involve certain private data. Because data does not have value in of itself, only when used to increase efficiency of actions, the condition for necessity raises questions. The only situation where private data can be more predictably necessary, is when a public sector body needs to fulfil a task in the public interest, grounded in law. Included in the need for the public sector body to "demonstrate" an exceptional need, cf. Article 14(1), is the demonstration of the data to be necessary.

It is not only the data which must be necessary to tackle the situation which decides when a request is proportionate. To achieve a regulation which is "fair", as suggested in the Data Act's title, and reasonable data exchange between businesses and the public sector body, the burden put on businesses should also be considered. In the context of Chapter V, the interests of the public sector body and the business receiving the request should be considered and weighed against each other. Article 15 does not outright state that such an evaluation should be taken into considered. But the emphasis of fair exchange in the preface of the Act can supplement our interpretation of Article 15. The public sector body should consider the business "legitimate interests".[77] One can make the argument that the current public opinion, general acceptance of a law and how authorities use it, should be a momentum when deciding what is

[75] Commission (2022): Data Act, explanatory memorandum p. 8.
[76] Commission (2022): Impact Assessment Report p. 34.
[77] Commission (2022): Data Act, recital 61.

a fair understanding in law.[78] But with regards for to the topic at hand, which is exceptional situations, the public may not be the best judge of what is fair, as the public can have a clear self-interest in the data transfer. Therefore, whether the data request is proportionate should be determined in the concrete situations where requests are made. As will be shown in Section 4.3.2, Article 18(2) allows the business receiving the request to refuse the transfer, and quite freely argue as to why the transfer would be disproportionate.

The statement in Article 14(1) "upon request the data holder shall make data available" is not entirely accurate. Even if a public sector body cannot demonstrate that there is an exceptional need for the requested data, an absolute obligation to transfer data at request is not present. Article 14(1) should be viewed in context with Article 18(2) which provide businesses possibilities to reject the transfer. But the main rule is still that the business must comply with the request. The wording of obligation in Chapter V cannot be interpreted as an absolute duty for the contacted business.

It is the institution requesting the data which must prove that there exists an exceptional need, the requirement for adequate evidence is outlined in Section 4.3.1. Naturally, it's also the institution which decides if there exists an exceptional need. When the public sector bodies decide to request a transfer in accordance with Article 14, they will be allowed a margin of appreciation. As showed in Section 1.2, when altering the property rights of a business, the public sector body must respect the Charter of Fundamental Rights. But even if the Data Act is passed as a regulation and not a directive, the Member States should have some flexibility in how they interpret Article 15 of the Data Act. Although, the conditions set in Article 15 can alone ensure that a lawful request will almost always be considered reasonable and proportionate. The conditions presented in Article 15, combined with the conditions presented in Articles 17-19 about requirements for appropriate transfer, are themselves meant to secure proportionate.[79]

4.3 Articles 17–19: Conditions for data request and storage.

[78] Schartum (2020), p. 89.

[79] Commission (2022): Data Act, explanatory memorandum p. 15.

Articles 14 and 15 are what determines when the request itself is legitimate. Articles 17-19 are important for understanding how a business can respond to the request. These Articles contain the second link of conditions which must be fulfilled for a request for data transfer in Chapter V to be legitimate as obligatory, with the conditions in Articles 14 and 15 being the first link. Should a public sector body demand data transfer from a business, the sector body will have certain responsibilities regarding the request of the data, ensuring data security, deletion, etc.

When a public sector body makes a request for a transfer of data it must, inter alia, "demonstrate the exceptional need", "state the legal basis" for the request and "explain the purpose of the request" (cf. Article 17(1)). Article 17(1) and (2) consists of rules for how a data request should be made by the requesting institution. The public sector body must demonstrate that there is an exceptional need for certain data, that the request is reasonable, proportionate, etc. While Article 17 sets conditions for legitimate request, Article 19 addresses how public sector bodies must handle the data after receiving it. It addresses inter alia use in accordance with purpose, "technical and organisational measures" for security and deletion (cf. Article19(1)(a-c)). Finally, Article 18 has a deadline for businesses to transfer requested data and addresses how a business can decline the request.

4.3.1 Formal conditions for transfer

A rule of note appears in Article 17(1)(e), which asks the requesting institution to present a deadline for transfer or for the business to express a wish for the requesting institution's to "modify or withdraw" the request for transfer. Nonetheless, a data holder must deliver the data "without undue delay" (cf. Article 18(1)). If the business decides to request a modification or withdrawal, the minimum deadline is "5 working days" if the requesting institution has claimed the exceptional need to be an emergency, otherwise its 15 working days (cf. Article 18(2)).

There are stricter conditions for certain categories of data. Trade secrets should only be requested to be transferred when "strictly necessary" and "appropriate" measures to secure the confidentiality of trade secrets must be taken, (cf. Article 19(2)). As mentioned, trade secrets are defined in the Trade Secret Directive Article 2(1). Interestingly, such protection is not given to intellectual property, even though the Data Act gives consideration towards

approving, as a main rule, data as intellectual property. Article 19(2) can hardly be used analogically to include intellectual property or other special categories of data, as the wording is too specific. Important non-personal data can be given special care as well, with basis in Article 17(2)(c); the public sector body shall "respect the legitimate interests" of the business, and the previously discussed proportionality with regards to the business' interests in Section 4.2.

When making a request in accordance with Article 14, the public sector body shall make the request available "online without undue delay" (cf. Article 17(2)(f)). Such documentation and openness should guarantee that there is no confusion about what was requested, should later disputes arise. The duty to report to the business when the data is destroyed pursuant to Article 19(1)(c) gives the business an overview. In the case of a public emergency, which should be national news, the business can more easily have control of when it can expect the data to be deleted.

The Data Act demands the designation of "one or more competent authorities" responsible for the "enforcement" of the Act (cf. Article 31(1)). The authorities shall handle complaints arising from "violations of this Regulation" (cf. Article 31(3)(b)). Legal persons have the right to lodge complaints with the "competent authority" (cf. Article 32(1)). If the business has suspicions that the public sector body(s) keep the data for a disproportionate amount of time, it may lodge a complaint to the competent authority pursuant to Article 32(1).

4.3.2 Right to request modification or withdrawal or a request for transfer

The right to request a modification or withdrawal of a request as mentioned in Section 3.4.1, must be justified on the grounds of the data either being "unavailable" or because the request "does not meet the conditions laid down in Article 17(1) and (2)" (cf. the Data Act Article 18(2)(a) and (b) respectively.

Unavailable is not defined in the Data Act. It would probably entail that it's out of the business' power to transfer the requested data. There can be a fault in electronic communication, an internal error in the database of the business or perhaps the business has sold the data without the public sector body knowing.

Article 18(2)(b) is open to arguments based on discretion. It can be argued whether the requesting public sector body has demonstrated an "exceptional need", a fitting "legal basis", whether the request is "proportionate to the exceptional need" and if it respects "the legitimate aims of the data holder" (cf. Article 17(1)(b) and (d), and (2)(b) and (c)) respectively. These provisions allow the business receiving the request to give an elaborate, argumentative explanation as to why it refuses to transfer the requested data.

The "data holder" can decline or seek modifications to a request for data to respond to a "public emergency" if the holder has already given the data to another public sector body for the "same purpose" as presented by the new data request, and the data holder has not been notified of the destruction of the previously requested data in accordance with Article 19(1)(c) (cf. Article 18(3)).

One may question if the right to decline a data transfer when the data has already been given for only one of the five exceptional situations in Article 15 fulfils the Once-Only principle, which is supposed to be respected.[80] Besides, giving businesses the right to decline a transfer in accordance with Article 18(3) for all of the exceptional situations would help the public sector bodies respect the "cost and effort" mentioned in Article 17(2)(c), which a business expends to fulfil the request.

4.3.3 Safeguards for data after transfer

4.3.3.1 Responsibilities of public sector bodies after data transfer

A public body sector which receives data due to a request "made under Article 14" shall not use the data in a manner which is "incompatible" with the given purpose of the request (cf. Article 19(1)(a)). The choice of using "incompatible" instead of demanding that the public sector body only use data in a way which is compatible with the original purpose gives the public sector body some flexibility in how to use the data. Similarly, the GDPR Article 5(1)(b) also states that data shall not be processed (used) in a manner which is "incompatible" with the stated purpose. Whether a new purpose is incompatible with the given purpose(s) for processing is decided by discretion. Momentums to consider are potential links between the

[80] Commission (2022): Data Act, recital 61.

purposes, the context for the collection of data, consequences for the data subject and whether appropriate safeguards are in place (cf. GDPR Article 6(4) (a, b, d, and e)). Considering the that the public sector body shall make for the "legitimate interests" of the business, evaluating the consequences by including a new purpose is paramount.

The public sector body holding the data must implement, if necessary to protect non personal data, "technical and organisational measures" that "safeguard" the data subject which has personal data (cf. Article 19(b)). "Personal data" should in the context of the Data Act be understood as mixed data. Technical and organisational measures for the protection of personal data as well as "data subject" is borrowed from the GDPR. As Article 19(1)(b) involves personal data, the understanding in the GDPR of appropriate measures can be fully relevant. What constitutes appropriate technical and organisational measures in the GDPR is too comprehensive to summarise here. Typical measures are data minimisation, not using more data than necessary, and encryption and anonymisation, which are mentioned in the Data Act.

Data which a public sector body has received from a business should be destroyed once keeping the data is "no longer necessary for the stated purpose" (cf. Article 19(1)(c)). Of note is that the public sector body specifies a "deadline", an exact date for the transfer of data, but must only state the intended duration of use (cf. Article 17(1)(c) and (e)). The public sector body can't know exactly when the purpose is fulfilled. Usually, the longer into the future one tried to predict; the more inaccurate a given time will be. Once again, the GDPR has a similar paragraph, namely Article 17, but with a few key differences which lessens its analogical use. Article 17 lists several situations which obliges the data controller to delete the data, while Article 19 only obliges deletion when the use of the data is fulfilled, apparently leaving deletion in control of the public sector body. The business can request and argue for a modification of the duration of the use (cf. Article 17(1)(c)). If the data has already been transferred, then the business can choose to lodge a complaint to a competent authority if it means that one of its rights "under this regulation" has been infringed (cf. Article 32(1)).

Regarding emergencies, the data would likely be destroyed when the data has been used by the public sector for addressing the crisis. In other words, when the data has effectively been applied with desired results. If the becomes apparent that the data cannot be meaningfully used, it should also be deleted. Otherwise, for other exceptional situations, the data should at latest be destroyed when the "specific task" mentioned in Article 15(c) is completed.

We can use the time of Covid-measures to show how difficult it is to find a common measurement of when an emergency is over, or what a pandemic even is. Different countries do not even have the same legal definition on epidemics. The World Health Organisation had still not declared the Covid outbreak over as of 14.09.2022,[81] but is this decisive for understanding the end of a health emergency in the context of the Data Act? As public sector bodies are national institutions, national law and policy will dictate what is a health emergency unless the nation in question has adopted relevant and overruling international law.

Article 17(3) states that the requesting institution should not make data available for "reuse within the meaning of Directive (EU) 2019/1024" (Open Data Directive). In the Open Data Directive, reuse of data means a party other than the public sector body use data held by it for purpose other than the purpose for which the data was produced (cf. the directive's Article 2 (11)(a)). This is understandable, as the data which can be reused according to the Open Data Directive is of such a character that one would not want to keep the data private, unlike for example personal data, intellectual property, and trade secrets. At the same time, Article 17(3) states that the Open Data Directive do not apply to "public sector bodies" that obtained the data in accordance with Chapter V. This should be read together with Article 17(4): a public sector body can share data with other institutions to complete the tasks in Article 15. This allows for sharing of data which can be necessary to uphold the Once-Only-principle. Obligations in Article 19 applies to the party receiving the data from the public sector body (cf. Article 18(4)).

4.3.3.2 Trust in the public sector amongst businesses and potential risks due to transfer of data Tie this to Section 4.3.3.1

A total of 75.7 % of stakeholders in businesses were concerned with a lack of "safeguards" ensuring that the data would only be used for the given "public interest purpose".[82] The Data Act cannot mend the clear lack of trust businesses have towards the public sector. The question is if the Act's conditions and accountability for public sector bodies is sufficient for the businesses to judge it as acceptable to transfer.

[81] UN news (2022), The end of the Covid-19 pandemics is in sight: WHO.

[82] Commission (2022): Impact Assessment Report, p. 19.

The responsibilities a public sector has regarding the confidentiality and integrity of transferred data dampen the risk businesses are forced to take when transferring data and should help with some of the trust issues which several stakeholders have voiced. The obligation to delete data when the purpose is fulfilled will limit the window for potential cyber-attacks which can reveal crucial business data. But Chapter V also allows for the requesting of a transfer of data that can reveal trade secrets. It also allows sharing of data between public sector bodies, which increases the risk of leakage, though which may be necessary to substantially save administrative costs

There is, however, a lack of certain safeguards in the Data Act which can legitimise the suspicions businesses may have. Corruption, cyber-attacks, and reverse engineering from competitors are some of the issues which can make businesses weary.

The main reason data transfer poses an increased threat of cyberattack is because the attacker now has one or more additional networks or databases to attack. Observational attackers will recognise that data can be transferred, exactly because the request for transfer will be published online by the public sector body making the request.

Business competitors can be looking for trade secrets and other private data. Competitors can see how the government chooses to implement the transferred data. They may analyse how the public sector chooses to use the newly transferred data. By reverse engineering the use of the data, they may get a better understanding of what the data is. However, there should already be multiple ways for rival businesses to observe how their competitors implement their data before such a transfer. The relatively brief public use of the data should not be a serious risk for the business from which the data is transferred.

4.4 Summary of public sector bodies' ability to request data and legal certainty

Stakeholders invited to give their opinion on the business-to-government data sharing presented in Chapter V have argued that public interest should be "clearly defined" and have laid

out “use-cases”, a sentiment which was supported by the Regulatory Scrutiny Board.[83] an advisory body within the Commission. Furthermore, public sector bodies have been cautious in utilising business-to-government data sharing due to legal uncertainty.[84] This decade has so far been a time of crisis. Certain public sectors in Europe may try to abuse the Data Act by declaring a crisis when it is doubtful that the country is in a state which fits the understanding of public emergency in the Act.

That several public sector bodies will attempt to misuse the Act is possible.[85] One question is therefore if there is sufficient legal certainty in Chapter V. When interfering with the rights of private parties, there should be a level of legal certainty so that the private parties can predict what is expected of them. The principle of legal certainty has been laid out by the CJEU. In Case C-81/10 *Francé Télécom v European Commission* para. 100 it was stated that the law should be “clear and precise and predictable” so parties can “ascertain their position in legal relations”.

First, it is worth mentioning how prime legal sources regulate legal certainty when the intervention in a right is possible. As a treaty, the Charter of Fundamental Rights is a binding legal force (cf. the Treaty of the European Union Article 6(1)). The Charter is binding for Member States insofar as they implement Union law (cf. the Charter Article 51(1)). The Charter “reaffirms” the “international obligations”[86] laid out in the Convention for the Protection of Human Rights and Fundamental Freedoms and should be interpreted in accordance with the “meaning and scope” there of (cf. the Charter of Fundamental Rights Article 52(3)).

The conditions in Article 15 are stern to such an extent that there is clearly a high threshold for enacting an obligatory transfer of data in accordance with the Act, including in the case of public interest. However, to make the Data Act easily adaptable to different national laws and situations, some of the conditions are ambiguous. Unfortunately, this also reduces the legal certainty for the business which may have to fulfil an obligation to transfer data, to such an extent that it makes the Act’s Article 14 unfit as a legal basis for requesting transfer. Many legal bases are open for discretion without this alone rendering the legal basis unfit.

[83] Ibid., p. 80 and 91.

[84] Commission (2022): Data Act, explanatory memorandum p. 10.

[85] Godel et a. (2022), p. 26.

[86] Council and Parliament (2012): Charter of Fundamental Rights of the European Union, preamble.

The terms public emergency and public interest could benefit for more description in the Data Act itself. Interpretation of public emergency could be more precise by granting concrete numerical measurements where this is natural. Public interest has been interpreted in other Union legal sources, such as the CJEU. Still, more elaborate clarification on the extent of public interest in the context of the Data Act would be welcomed.

The many formal conditions for requesting a transfer in Article 17(1) and (2), especially the deadline, means that the business will not be too overwhelmed and can consider their options. The conditions in Article 17(1)(b) and (c) which together implies that the requester must argue why the data acquisition is necessary to respond to an exceptional situation, means that the process should not be arbitrary, but predictable.

The ways in which a business can respond to a request for transfer makes the usability and outcome of a data request even more insecure. But that element of uncertainty come from a part of the process which is to the benefit of the business. It does therefore not increase the legal uncertainty which can make Article 14 a legal basis with inadequate legal certainty.

The public sector bodies possibility of acquiring data is overall quite slim because of the stern conditions in Article 15 and the multiple ways in which a business can object to the proposed transfer found in Article 18(2). While not being unfit as a legal basis due to legal uncertainty, it is highly recommended that some of the ambiguity in Chapter V becomes more precise. One possibility would be to change purpose limitation in Article 19 so that the public sector body can only use the data for the "explicitly requested purpose".[87]

5 Implications of Chapter V of the Data Act for businesses

Much of the content in Chapter V of the Data Act is explained in Section 4, but the question of what the economic consequences of Chapter V are for businesses is not fully answered. There are several aspects that should be discussed. This chapter is focused on the potential for legal disputes rooted in Chapter V, when a business can expect compensation for a data transfer and potential benefits businesses can acquire due to the obligation to transfer data in

[87] Godel et al. (2022): p. 26.

Article 14 of the Data Act. All these questions have an economical aspect, and they should be answered to better understand whether the economic burden placed businesses due to an obligation to transfer data is acceptable. The actual costs and benefits will only be apparent ex post of the possible acceptance of the Data Act, but there is enough information now to make predictions.

5.1 Legal disputes

In the case of obligatory transfer, the possibility for costs tied to legal disputes is quite possible. The right of a business to refuse a transfer in the Data Act Article 18(2) allows for numerous situations where the parties can argue whether an obligation to transfer is present.

Court cases unfortunately cost everyone involved time and often a significant sum of money. If the obligatory data transfer is instilled there will be court cases which are part of the equation for judging whether the data transfer will be a societal boon or burden.

The competent authorities will dampen the costs associated with legal disputes. The possibility of costly court cases exists but is slim per legal dispute. The legal costs can therefore be expected to be manageable. As Chapter V only targets businesses bigger than "small" as defined in Recommendation 2003/361/EC, most affected businesses can comfortably tackle disputes from an economic standpoint.

5.2 Article 20: Compensation in case of exceptional need

If the obligation to transfer data stems from a need to "respond to a public emergency", an ongoing crisis, the affected business may not demand compensation (cf. the Data Act Article 20(1)). On the contrary, in the case of prevention or recovery from a public emergency, or the transfer of data is due to public interest, a business can claim compensation for the costs of the data transfer (cf. Data Act Article 20(2)). The compensation shall make the transfer a net-zero cost for the business. The five situations in Article 15 differs regarding the question of compensation to businesses for the costs tied to a transfer of data.

The divide in compensation between a response to public emergencies and all other exceptional situations is not explained in the Data Act, but it emphasises the importance of addressing public emergencies, as if this justifies the transfer of data without compensation.[88]

What form of compensation the enterprise can expect is of great importance for evaluating obligatory data transfer from the business' perceptive, presuming that they main goal of the business is profit. Making the response free of charge but granting compensation for preventing a public emergency does not incentivise the public sector to focus on prevention, regardless how small the transfer cost may be. Furthermore, it would be reasonable to cover the costs of the business which must allow public sector bodies to borrow its private data. A business would also find reason for making necessary digital infrastructure investments for safe transfer if it was guaranteed "adequate compensation".[89]

Regarding the amount that will be compensated, the public sector's compensation will not exceed "technical and organisations costs incurred to comply with the request" (cf. Article 20(2)). This includes compensation for the digital infrastructure costs and security measures. Worth noting is that Article 20 does not give directly give compensation for lost profit due to manpower used to complete appropriate transfers. Meeting high-quality standards for data can be costly.[90] Including compensation for all exceptional situations, the public sector should provide compensation for the manpower resources a business uses to comply.

5.3 Reduction of costs for businesses

This proposal will give rise to administrative costs. These are to be borne mainly by the public sector and the affected businesses. However, the exploration of different options and their expected costs and benefits in the Data Act's supporting papers should help to minimise unnecessary costs. Furthermore, the costs can be counterbalanced by the value to be derived from broader access and use of data, as well as the market uptake of novel services.[91]

[88] Commission (2022): Data Act, recital 67.
[89] Godel et al. (2022), p. 23.
[90] Ibid., p. 23.
[91] Commission (2022): Data Act, explanatory memorandum p. 9.

As mentioned in Section 2 and Section 3.1, the Union data legislation is predicted to benefit the economy in the internal market, and a significant part of the benefit is for businesses. The Data Act should not be different in this regard.

One can argue that because a single coherent set of EU rules is great for the single market and therefore for European commerce, which counterbalances the cost for businesses for copying with request for transfer in accordance with Chapter V. Even if obligatory data transfer is unreasonable for businesses, it's better to have a predictable, common set of rules then several fragmented ones, which currently is a problem as mentioned in Section 3.1.

6 Conclusion

In this paper I have tried to make Chapter V of the Data Act proposal, as well as reasons for the proposal and consequences of it more comprehensive. I have done this using scrutiny of the legal text, especially the conditions for data transfer, context, and relationship with other Union legislation. Most request for data transfer in accordance with the Data Act Article 14 will be deemed as reasonable and fair, simply by the nature of the exceptional situations under which the request can be made. This alone will often be enough to conclude that a data transfer is justifiable. There will also be, however, several edge cases in the question of transfer, both in terms of what is legal and what is beneficial. This edge cases be particularly relevant if one of the exceptional situations in Article 15(c) is used as a legal basis.

All the exceptional situations in Article 15 have not insignificant ambiguity. Contrary to the aim stated in the explanatory memorandum regarding the Data Act, Chapter V somewhat fails to be a "predictable" [92] mechanism to tackle the exceptional situations in Article 15. Combined with the possibility for a receiving business to reject the requested data transfer with an objection based in Article 18(2)(b), which opens for a defence of the rejection by attacking the vague conditions for the request, we can expect several legal disputes. As with the legal implications of the GDPR, the ambiguity will likely be resolved in cases brought before the CJEU.

[92] Commission (2022): Data Act, explanatory memorandum p. 2.

The risk and costs businesses will receive due to Chapter V of the Data Act are acceptable, but not as proportionate as they could be. It is unclear how consistently the data transfer in accordance with Article 14 will be a net benefit. Poor decisions within public sector bodies, manpower used to deliver data in accordance with the Data Act's standards, a bit too ambiguous conditions in Chapter V, and resources spent in negotiations and legal disputes can make the costs greater than the benefit. More precise and rigid conditions for data transfer in Chapter V would help to reduce the costs.

Bibliography

Cases

Case C-454/18 *Baltic Cable*	ECLI:EU:C:2020:189
Case C-266/96 *Corsica Ferries France SA*	ECLI:EU:C:1998:306
Case C-136/04 *Deutsches Milch-Kontor GmbH v Hauptzollamt Hamburg-Jonas*	ECLI:EU:C:2005:716
Case C-81/10P *Francé Télécom v European Commission*.	ECLI:EU:C:2011:811
Case C-242/95 *GT-Link A/S*	ECLI:EU:C:1997:376
Case C-108/09 *Ker Optika*	ECLI:EU:C:2010:725
Case C-179/90 *Merci convenzionali porto di Genova*	ECLI:EU:C:1991:464
Case C-306/12 *Spedition Welter*	ECLI:EU:C:2013:359
Case C-621/18 *Wightman*	ECLI:EU:C:2018:999

Laws and charters

Charter of fundamental rights	*Charter of Fundamental Rights of the European Union*, 26.10.2012, C 326/02
European Convention of Human Rights	*Convention for the Protection of Human Rights and Fundamental Freedoms*, Rome, 04.11.1950.
Data Act	*Proposal for a regulation of the European Parliament and of the Council on European harmonised rules on fair access to and use of data (Data Act)*, Brussels, 23.2.2022, COM(2022) 68 final.
Database directive	*Directive 96/9 EC of the European Parliament and of the Council of 11. March 1996 on the legal protection on databases*, 27.3.1996, L 77/20.
Data Governance Act	*Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act)*, Brussels, 25.11.2020, COM(2020) 767 final.

Free-flow regulation	*Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union*, 28.11.2018, L 303/59.
General Data Protection Regulation	*Regulation (EU) 2016/679 of the European Parliament and 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 (General Data Protection Regulation)*, Brussels, 04.05.2016, L 119/1.
Open data directive	*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 (recast)*, 26.6.2019, L 172/56.
Protocol of the European Convention of Human Rights	*Protocol to the Convention for the Protection of Human Rights and Fundamental Freedoms*, Paris, 1952.
Treaty of the European Union	*Consolidated Version of The Treaty on European Union*, 7.6.2016, EUT 2016/C 201/1.

Treaty on Stability, Coordination and Governance	*TREATY ON STABILITY, COORDINATION AND GOVERNANCE IN THE ECONOMIC AND MONETARY UNION BETWEEN THE KINGDOM OF BELGIUM, THE REPUBLIC OF BULGARIA, THE KINGDOM OF DENMARK, THE FEDERAL REPUBLIC OF GERMANY, THE REPUBLIC OF ESTONIA, IRELAND, THE HELLENIC REPUBLIC, THE KINGDOM OF SPAIN, THE FRENCH REPUBLIC, THE ITALIAN REPUBLIC, THE REPUBLIC OF CYPRUS, THE REPUBLIC OF LATVIA, THE REPUBLIC OF LITHUANIA, THE GRAND DUCHY OF LUXEMBOURG, HUNGARY, MALTA, THE KINGDOM OF THE NETHERLANDS, THE REPUBLIC OF AUSTRIA, THE REPUBLIC OF POLAND, THE PORTUGUESE REPUBLIC, ROMANIA, THE REPUBLIC OF SLOVENIA, THE SLOVAK REPUBLIC, THE REPUBLIC OF FINLAND AND THE KINGDOM OF SWEDEN T/SCG/en 1 THE KINGDOM OF BELGIUM, THE REPUBLIC OF BULGARIA, THE KINGDOM OF DENMARK, THE FEDERAL REPUBLIC OF GERMANY, THE REPUBLIC OF ESTONIA, IRELAND, THE HELLENIC REPUBLIC, THE KINGDOM OF SPAIN, THE FRENCH REPUBLIC, THE ITALIAN REPUBLIC, THE REPUBLIC OF CYPRUS, THE REPUBLIC OF LATVIA, THE REPUBLIC OF LITHUANIA, THE GRAND DUCHY OF LUXEMBOURG, HUNGARY, MALTA, THE KINGDOM OF*

	THE NETHERLANDS, THE REPUBLIC OF AUSTRIA, THE REPUBLIC OF POLAND, THE PORTUGUESE REPUBLIC, ROMANIA, THE REPUBLIC OF SLOVENIA, THE SLOVAK REPUBLIC, THE REPUBLIC OF FINLAND AND THE KINGDOM OF SWEDEN, 02.03.2012.
Treaty on the Functioning of the European Union	*Consolidated Version of the Treaty on the Functioning of the European Union*, 26.10.2012, TFEU 2012/C 326/47.

Reports, guidelines, impact assessments, policy documents and other official documents

A European Strategy for data (2015)	European Commission. Communication from the commission to the european parliament, the council, the european economic and social committee and the committee of the regions - *A Digital Single Market Strategy for Europe*, Brussels, 6.5.2015. COM(2015) 192 final.
Concerning the definition of small, micro and medium-sized enterprises (2003)	European Commission. *Commission Recommendation of 6 May 2003 concerning the definition of small, micro and medium-sized enterprises*, Brussels, 20.05.2003, L 124/36.
Council Decision (2014/415/EU)	European Council. *Council Decision of 24 june 2014 on the arrangements for the implementation by the Union of the solidarity clause* (2014/415/EU), 1.7.2014, L 192/53.
Dutch-Brown and Martenes (2020)	Néstor Dutch Brown and Bertin Martenes. *JRC Digital Economy Working Paper 2020-04, The economics of Business-to-Government data sharing*, 2020.
Executive Summary of the Impact Assessment Report	European Commission. *Commission staff working document executive summary of the impact assessment*, Brussels, 23.02.2022, SWD (2022) 34 final.

Public consultation on the Data Act (2021)	European Commission. *Public Consultation on the Data Act*, 2021.
Recommendation 2003 361/EC	European Commission. *COMMISSION RECOMMENDATION of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises*, 20.05.2003, L 124/36.
Shaping Europe's digital future (2020)	European Commission. Communication From the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – *Shaping Europe's Digital Future, Brussels*, 19.2.2020 COM(2020), 67 final.
Study in support of the evaluation of Directive 96/9/EC on the legal protection of databases	European Commission. *Study in support of the evaluation of Directive 96/9/EC on the legal protection of databases, prepared for DG CNECT by JIIP and Technopolis Group*, 2014.
Towards a European strategy on business-to-government data sharing for the public interest (2020)	European Commission, Directorate-General for Communications Networks, Content and Technology. *Towards a European strategy on business-to-government data sharing for the public interest Final report prepared by*

	the High-Level Expert Group on Business-to-Government Data Sharing, 2020.
Towards a thriving data-driven economy (2014)	European Commission. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the regions towards a thriving data-driven economy,* Brussels, 2.7.2014, COM(2014) 442 final.
Impact Assessment Report (2022)	European Commission. *Commission Staff Working Document Impact Assessment Report Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data* (Data Act), Brussels, 23.2.2022 SWD (2022) 34 final.
Study to support an Imapact Assessment (2022)	Denny, Emily, Marie Eichholtzer, Hans Graux, Franziska Hoerth, Eike-Christian Koring, David Osimo, Angeliki Papadimitriou, Sebastiaan van der Peijl, Cristina Moise, Marc Nikolov, David Osimo, Claire Stolwijk Cleónice León Vargas, Stefaan Verhulst, Alan Walker and Mahlet Zimeta. *Study to support an Impact on enhancing the use of data in Europe*, 2020.

Articles and research papers

Bealoup et al. (2021)	Bealoup, Julia, Emre Bay, Aliki, Benmayor, Charlotte Ducuing, Lidia Dutkiewicz, Teodora Lalova, Yuliya Miadzvetskaaya and Bert Peters. *White Paper on the Data Governance Act*, 2021.
Brooks (03.06.2022)	Brooks, Chuck. *Alarming Cyber Statistics for Mid-Year 2022 That You Need To Know*, 03.06.2022.
Chu (2022)	Chu, Jingyi. *Chapter 5 of the Data Act – Which should be the legal basis for B2G data sharing: "exceptional need" or "public interest"?*, 2022
Duch-Brown and Martens (2020)	Néstor Duch-Brown and Bertin Martens. *The economics of Business-to-Government data sharing*, 2020.
Efroni et al. (2022)	Efroni, Zohar, Prisca von Hagen, Peter Robert, Mariam Sattorov and Lisa Völzmann. *Position paper regarding Data Act (Proposal of the European Commission), (23.02.2022)*, 2022.

Godel et al. (2022) — Godel, Moritz, Pietro Guglielmi, Victoria Harris-Honrado, Gordon Moir, Clio von Petersdorff and Sam Wood (Etno). *Study on the impact of the Data Act proposal on European telecom operators*, 2022.

Iacus et al. (2021) — Iacus, Stefano Maria, Carlos Santamaria, Francesco Sermi, Spyridon Spyratos, Dario Tarchi and Michele Vespe. *On the Use of Data from Multiple Mobile Network Operators in Europe to fight COVID-19*, 2021.

Graef and Husovec (2022) — Inge Graef and Marin Husovec. *Seven things to improve the Data Act*, 2022.

ODI, The GovLab, Cuebiq (2021) — ODI, The GovLab, Cuebiq. *The Use of Mobility Data for Responding to the COVID19 Pandemic*, 2021.

Menisk (2022) — Mensik, Hailey. *Healthcare cyberattacks led to worse patient care, increased mortality, study finds*, 08.09.2022.

Micheli (2022) — Marina Micheli. Public bodies access to private sector data: *The perspectives of twelve European local administrations*, 2022.

Namasudra (2018)	S. Namasudra. *Cloud Computing: A New Era*, 2018.
Öjehag-Pettersson and Padden (2021)	Andreas Öjehag-Pettersson and Michaela Padden. *Protected how? Problem representations of risk in the General Data Protection Regulation (GDPR)*, 2021.
Tarkowski and Vogelez (2022).	Alex Tarkowski and Francesco Vogelez. *Data Act: business to government data sharing*, 2022.
UN news (2022) The end of the Covid-19 is in sight: WHO.	UN news. *The end of the Covid-19 pandemic is in sight*, 2022.

Books

Arnesen, Kolstad, Rognstad and Sejersted (2014)	Arnesen, Finn, Olav Kolstad, Ole-Andreas Rognstad and Fredrik Sejersted. *EØS-rett, issue 3*, 2014.
Bassett, Marris and Thornham (2009)	Basset, Caroline, Paul Marris and Sue Thornman. *Media Studies A Reader Third Edition, issue 3*, 2009.
Bradford (2020)	Bradford, Anu. *The Brussels Effect*, 2020.
Eide and Stavang (2018)	Erling Eide and Endre Stavang. *Rettsøkonomi, issue 2*, 2018.
Schartum (2020)	Dag Wiese Schartum. *Personvern-forordningen – en lærebok*, 2020.

Webpages:

European Union	**https://european-union.europa.eu/index_en¨**