MASTER THESIS

Titel der Master Thesis / Title of the Master‘s Thesis

„ Dispute Resolution under the EU Data Act“

verfasst von / submitted by

Amarilda Ulrich

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of

Master of Laws (LL.M.)

Wien, 2023 / Vienna 2023

Studienkennzahl lt. Studienblatt / Postgraduate programme code as it appears on the student record sheet:	UA 992 548
Universitätslehrgang lt. Studienblatt / Postgraduate programme as it appears on the student record sheet:	Europäisches und Internationales Wirtschaftsrecht / European and International Business Law
Betreut von / Supervisor:	Janet Martinez, PhD, MPA, JD, BS

Abstract

The EU Data Act is a proposal for a regulation published in February 2022. Such a regulation will enable mandatory non-personal data sharing between data holders, users, and recipients (as per the user's request). The data to be shared is the data that will be generated from an IoT device or related service. Moreover, it will facilitate switching between cloud processing service providers. As it is one of the most comprehensive attempts from the EU to mandate data sharing between market participants, there is a lot of interest, uncertainties, confusion, and not enough research in this area. Many authors have researched certain topics (such as user rights, etc.), but not many have been focusing on the potential disputes that might arise, and how to manage and resolve those disputes. The research method used for this paper is qualitative research. The author has consulted EU laws, literature, articles, and opinions of academics and different stakeholders, to help clarify the Data Act concepts and procedure to be followed upon entry into force. Research has shown that more certainty is needed, especially on rules for the sharing of trade secrets, personal data (mixed data sets), and how to resolve potential disputes that might arise. Regarding dispute resolution, there are suggested three possible scenarios; provide clarity on existing designed dispute resolution systems, expand the scope of disputes to be handed by the dispute resolution body under article 10, or transfer the competencies of the dispute resolution body to competent authorities that will be responsible as per article 31 of the Data Act proposal.

Keywords: EU Data Act, user, data holder, mandatory data sharing, cloud switching, IoT device.

Abstrakt

Das EU-Datenschutzrecht ist ein Verordnungsvorschlag, der im Februar 2022 veröffentlicht wird. Diese Verordnung wird die obligatorische Weitergabe nicht personenbezogener Daten zwischen Dateninhabern, Nutzern und Empfängern (je nach Wunsch des Nutzers) ermöglichen. Bei den zu teilenden Daten handelt es sich um Daten, die von einem IoT-Gerät oder einem damit verbundenen Dienst erzeugt werden. Auch der Wechsel zwischen Anbietern von Cloud-Diensten soll erleichtert werden. Da es sich um einen der umfassendsten Versuche der EU handelt, den Datenaustausch zwischen Marktteilnehmern zu regulieren, gibt es in diesem Bereich viel Interesse, Unsicherheit, Verwirrung und noch zu wenig Forschung. Viele Autoren haben sich mit spezifischen Themen beschäftigt (z.B. Nutzerrechte usw.), aber nur wenige haben sich auf mögliche Streitigkeiten konzentriert, die entstehen können, und darauf wie diese Streitigkeiten gehandhabt und gelöst werden können. Die für diese Arbeit verwendete Forschungsmethode ist die qualitative Forschung. Die Autorin hat EU-Recht, Literatur, Artikel und Meinungen von Wissenschaftlern und verschiedenen Interessengruppen konsultiert, um Konzepte und Verfahren des Datenschutzgesetzes zu klären, die bei Inkrafttreten zu befolgen sind. Die Untersuchungen haben gezeigt, dass mehr Sicherheit insbesondere bei den Regeln für die Offenlegung von Geschäftsgeheimnissen, von personenbezogenen Daten (gemischte Datensätze) und der Beilegung potenzieller Streitigkeiten erforderlich ist. Im Hinblick auf die Streitbeilegung werden drei mögliche Szenarien vorgeschlagen: Klärung der bestehenden Streitbeilegungssysteme, Erweiterung des Anwendungsbereichs der Streitbeilegungsstelle nach Artikel 10 oder Übertragung der Befugnisse der Streitbeilegungsstelle nach Artikel 10 auf die nach Artikel 31 der Datenschutzbestimmungen zuständigen Behörden.

Schlüsselbegriffe: EU-Datenschutzrecht, Nutzer, Dateninhaber, obligatorische Datenfreigabe, potenzielle Änderung, IoT-Gerät.

Table of Contents

Table of Abbreviations

ACEA	European Automobile Manufacturers' Association
ADR	Alternative Dispute Resolution
AI	Artificial Intelligence
BEUC	European Consumer Organization
CERRE	Centre on Regulation in Europe
CCIA	Computer & Communications Industry Associations
DA	Data Act
DGA	Data Governance Act
DSB (s)	Dispute Settlement Body (ies)
DSD	Dispute Settlement System
ECJ	European Court of Justice
ECO	European Consumer Organization
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
ELI	European Law Institute
EU	European Union
FRAND	Fair, reasonable and non-discriminatory
GDPR	General Data Protection Regulation
GDP	Gross domestic product
IoB	Internet of Behaviour
IoT	Internet of Things
IT	Information Technology
IP	Intellectual Property
MS	Member State (s)
NGO	Non-governmental organization
SEP	Standard Essential Patents
SMEs	Small Medium Enterprises
TSD	Trade Secrets Directive

Declaration of Academic Integrity

I hereby confirm that I prepared this Master Thesis independently and on my own, by exclusive reliance on the tools and literature indicated therein. The sources of other people's work have been appropriately referenced. Quotation marks are used around materials written verbatim from other sources.
The thesis has not been submitted to any other examination board.

Vienna, 30 August 2023

Amarilda Ulrich

Foreword

I would like to express my profound gratitude to my master's thesis supervisor, Janet Martinez. She provided me with invaluable guidance throughout this academic journey. Her experience and mentorship were instrumental in choosing a compelling research topic and shaping the direction of my thesis.

Moreover, she was always approachable, ready to provide constructive feedback and consistently ensure that her feedback was delivered promptly, allowing for the efficient progress of the thesis.

I am truly grateful for her support.

Vienna, 30 August 2023

Amarilda Ulrich

1 Introduction

This paper focuses on the European Union (EU) Data Act (DA). The DA is a proposal for a regulation that was published by the EU Commission in February 2022.[1] The piece of legislation will enable mandatory data sharing between different stakeholders. As it is the first legislation of its kind in the EU, and since we live in the area of technology and data is present in large parts of our lives, it is very important not only for academia but also for the wide range of stakeholders that will be affected by such law. At the moment of delivery of this paper, the DA is still a proposal, in the legislative phase and is expected to become law within 2023.[2]

From the moment it has been published, it has attracted the attention of a wide range of stakeholders for its controversies and the need for clarity, hence has become an object of research among academics. As it is a very recent topic, even though it is being researched by many academics, there is still not a lot of research available, especially in the area of dispute settlement and complaint handling systems designed in the DA proposal. Many authors have researched the impact that it will have, the rights of the user to the data, modalities for making data available, etc.

The purpose of this paper is to examine and analyze the DA proposal, identify potential problems, especially with regard to the disputes that are expected to arise, and resolving of these disputes (how, where, and what are the rules to be followed for resolving these disputes).

The research aims to answer the question: what kind of protocols, and information flows will help prevent, diagnose, and resolve the disputes arising from the EU Data Act? The research method used for writing this paper is qualitative research. The author has examined relevant literature, laws, books, articles, opinions, and assessments to help understand the DA proposal better and at times draw parallels with existing laws or procedures. The interpretations of different authors of the DA proposal have helped to better understand the issues related to the DA proposal and issue protocols and suggestions on how to manage certain disputes better.

[1] Commission, 'Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)' COM (2022) 68 final (EU Data Act Proposal).
[2] European Parliament, 'Data Act, Legislative Train Schedule' (*European Parliament,* 23 June 2023) <www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-data-act?sid=7101> accessed 21 July 2023.

This paper is structured in 8 different chapters. The first chapter is a short introduction to the topic (its importance) and the research question. The second chapter focuses on the background of the DA proposal, and what were the main incentives for the legislator for coming up with this proposal. Further, there is an explanation of the main points of the DA to understand what it is about, conditions, and mechanisms for data sharing and switching between data processing service providers. The third chapter identifies who are the stakeholders are and what is their position regarding the newly published DA proposal and what are their concerns regarding the proposal. The fourth chapter identifies and analyzes some of the problems of the DA proposal, problems which have been identified often and by different stakeholders or academics. The fifth chapter examines in detail two bodies that will have the role of dispute/complaint handling for the issues arising out of the DA proposal. There is a comparison between the DA proposal, the adopted text from the European Parliament (EP), and the adopted text from the Council, and what changes each of them suggests making in the proposal. Lastly, this chapter identifies some of the potential disputes that might arise under the DA proposal. The sixth chapter focuses on the flaws of the DA proposal and then analyzes the dispute settlement systems as per the framework provided by academics and suggests scenarios for providing clarity and having an effective dispute settlement system in place. There is chapter seven that summarizes the results, provides conclusions on the research, and recommendations for further research areas. Lastly, chapter eight captures all the resources used for this research.

The main findings consist of providing clarity regarding the sharing of trade secrets, personal data, what data shall be shared, rules on switching between cloud providers, etc. Regarding dispute resolution systems, the two designed systems at this stage have certain flaws. In order to avoid confusion and have an effective dispute settlement system, there are proposed three potential scenarios: provide clarity and/or transparency in the currently designed dispute resolution system, expand the scope of disputes specified in article 10 of the DA proposal, or transfer the DSB competencies (as designed in article 10) to ‘competent authorities’ designed under article 31 of the DA proposal.

2 Data Act Background

2.1 Legislative and policy purpose of the Data Act

EU DA is a proposal for a regulation suggested as part of the European data strategy.[3] It is the second horizontal legislation initiated based on that European data strategy published in 2020.[4] The EU DA comes as complementary legislation, following the EU Data Governance Act (DGA). European data strategy aims to empower data sharing in the era of a data-driven society. Its objective is to make the EU a leader in an area of technology, specifically a data leader, to set an example for the rest of the world, and to establish a system where the data flows freely within the EU area. Such a strategy intends to create a market where the data can be easily shared and utilized among different sectors of the economy, and different stakeholders (no matter the size), where each of them will have certain benefits and contributions.[5]

The volume of data being generated is growing every year. In 2018, the volume of data generated was 33 zettabytes. This amount is expected to reach 175 zettabytes in 2025. A large volume of this data (80%) generated is not being used, parts of it due to certain legal restrictions, technical and economic issues. The DA intends to enable businesses and individuals within the EU to use and reuse certain data. Such use is expected to boost the economy by creating EUR 270 billion of GDP increase by 2028 and drive innovation.[6]

A major driver for the DA is also the concerns of the EU on the dependency of EU businesses on non-EU businesses, especially in the area of cloud providers as there is low switchability between providers.[7] The European market has been seeing an increase in the participation of foreign cloud providers, especially US providers. According to a study published by Synergy Research Group in November 2022, it captures approximately three-quarters of the EU

[3] Commission, 'Data Act: Commission proposes measures for a fair and innovative data economy' (Press Release) (2022) <https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113> accessed 4 February 2023.
[4] Commission, 'Data Act - Questions and Answers' (Questions and Answers) (2022) <https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_1114> accessed 4 February 2023.
[5] Commission, 'Shaping Europe's digital future: Commission presents strategies for data and Artificial Intelligence' (Press Release) (2022) <https://ec.europa.eu/commission/presscorner/detail/en/ip_20_273> accessed 18 March 2023.
[6] Commission 'Data Act: Commission proposes measures for a fair and innovative data economy' (n 3).
[7] Commission, 'Accompanying Commission Staff Working Document - Impact Assessment Report', SWD (2022) 34 final, 24-25 <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022SC0034&from=EN> accessed 4 February 2023.

market.[8] Even though the European cloud market is much bigger now in comparison with five years ago (2017), its market share has dropped to 13% in 2022.[9]

Another purpose for introducing the DA surges from the developments in different Member States (MS). As MS have signed agreements with each other with regards to data sharing, as well as introduced national laws (such as France, Finland, etc.), hence the EU identified the need to unify the rules in order not to disrupt the single market.[10]

Given the nature of the data that may be generated by the IoT devices, where they may be generated mixed data sets (personal and non-personal data), the procedure for handling and rights on personal data is however clear and processing shall take place as specified under the General Data Protection Regulation (EU) 2016/679 (GDPR). Regarding non-personal data, the legal rights to data are not clearly specified and this can potentially allow the manufacturers of IoT devices to technically create/produce the device in a way and structure that enables them to exercise actual/practical control over the data produced by the IoT device.[11]

Furthermore, considering the market behavior, and the current situation where the largest holders of data are manufacturers (companies), another reason for this legislative initiative would be to regulate the behavior of the stronger actors in the market and set a balance between the party that exercises authority over the data and the party that might benefit from data.

Besides political and strategic reasons, the main goal of the DA proposal is to increase data flow within the EU (data generated by EU users, using EU or non-EU providers). Moreover, it intends to increase the volume of data and the speed of data sharing, so users and data recipients can effectively make use of data. In terms of data processing service providers, the goal of the proposal is to increase switchability so EU businesses can easily switch providers without seeing it as a burden on their business.

---

[8] 72% of the European Cloud Market is held by three American companies: Amazon Web Services, Microsoft Azure and Google Cloud.

[9] Synergy Research Group, 'European Cloud Providers Continue to Grow but Still Lose Market Share' (*Synergy Research Group,* 27 September 2022) <https://www.srgresearch.com/articles/european-cloud-providers-continue-to-grow-but-still-lose-market-share> accessed 4 February 2023.

[10] Commission, 'Commission Staff Working Document - Impact Assessment Report' (n 7) 25.

[11] Wolfgang Kerber, 'Governance of IoT Data: Why the EU Data Act will not fulfill its objectives' (2023) 72 (2) GRUR International <https://doi.org/10.1093/grurint/ikac107> accessed 29 April 2023.

2.2 Scope of the Data Act

The scope of the DA proposal is to establish a set of uniform rules regarding the share of data. The Regulation focuses on the following matters:

a. Manufacturer of devices[12] or related services shall make the data available to the user[13] of such devices or related services;

b. With the request or consent of the user, the data holder[14] shall provide/share the data with the data recipient[15];

c. The data holder should share the data with public institutions or institutions so the Union whenever the public emergency criteria are satisfied[16].

d. Data processing providers (i.e., cloud providers) should facilitate switching from one cloud provider to another one.[17]

The regulation intends to regulate the relationship and specify the rights and obligations of direct stakeholders, such as users of IoT devices or related services, data recipients, data holders (in the quality of manufacturers or suppliers), public institutions, Union institutions, and providers of cloud/edge services.[18]

In the most recent political agreement reached by the EP and Council, it is agreed that the rules set in this proposal shall apply to all providers that offer IoT devices or related services, to users within the EU, no matter where their place of establishment is. This will require all

[12] It can also be referred to as IoT devices. Recital 14 of the proposal provides some examples of what products may be subject to this regulation, such as vehicles, home equipment, medical and health devices, machinery, etc.

[13] EU Data Act Proposal, art 2 (5) defines the user as *'*a natural or legal person that owns, rents or leases a product or receives a services'.

[14] EU Data Act Proposal, art 2 (6) defines the data holder as 'a legal or natural person who has the right or obligation, in accordance with this Regulation, applicable Union law or national legislation implementing Union law, or in the case of non-personal data and through control of the technical design of the product and related services, the ability, to make available certain data'.

[15] EU Data Act Proposal, art 2 (7) defines data recipient as 'a legal or natural person, acting for purposes which are related to that person's trade, business, craft or profession, other than the user of a product or related service, to whom the data holder makes data available, including a third party following a request by the user to the data holder or in accordance with a legal obligation under Union law or national legislation implementing Union law'.

[16] Commission, 'Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)' COM (2022) 68 final (EU Data Act Proposal).

[17] ibid ch VI.

[18] ibid art 1 (2).

non-EU-based providers (including data processing service providers) to abide by these rules.[19]

2.3 What is data and what data can be shared under the Data Act?

> Article 2 (1) of the DA proposal defines the data as 'a digital representation of acts, facts, or information and any compilation of such acts, facts or information, including in the form of sound, visual or audio-visual recording'.[20]

The DA proposal intends to enable mandatory data sharing. The data that is to be shared is the data generated by an IoT device or related services. The DA proposal tasks the data holder (manufacturer or supplier when having control over the data) to ensure that users and data recipients have access to data and such data is provided in an accurate, reliable, complete, and up-to-date form.[21] The natural question that comes up in such a case, is what data must be shared. As extracted from the DA proposal, the data generated mainly refers to the raw data (not modified significantly or slightly modified to be made usable/readable) generated using the IoT device. Many claim that the definition of the data within the DA proposal is too broad.

In its adopted position on 17 March 2023, the Council of the EU suggests limiting the scope of application to not every data that is created by the IoT device but only to the data that is automatically derived by the use of IoT device or is slightly processed in order to be used by the user (i.e., formatting). The changes proposed by the Council in recital 14 (a) of the draft, specifically exclude from the scope of application the data that is significantly processed, and major changes are made to the raw data. The processed data is not a result of the actions or non-actions of users, but instead an outcome of the investments made by the data holder in relation to such data, hence such data is not subject to mandatory sharing.[22]

The upside side of a broad definition of data is that it may be inclusive of different/many sectors, as different IoT devices and related services may generate different data and in order

---

[19] European Parliament, 'Provisional agreement resulting from interinstitutional negotiations' (*European Parliament,* 14 July 2023) 57-58 <https://www.europarl.europa.eu/RegData/commissions/itre/inag/2023/07-14/ITRE_AG(2023)751822_EN.pdf> accessed 05 August 2023.

[20] EU Data Act Proposal, art 2 (1).

[21] ibid paras14 and 28.

[22] Council of the EU, '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) - Mandate for negotiations with the European Parliament' (Interinstitutional Negotiations) (2023) 7413/23, 10 <https://data.consilium.europa.eu/doc/document/ST-7413-2023-INIT/en/pdf> accessed 16 May 2023.

to cover all possible data to be shared with the user or the data recipient a broad definition would be helpful. Also, when the legislator drafts the laws, quite often it's almost impossible to capture all the variety and amount of data that the user may be entitled to receive. Moreover, with the rapid technological changes in today's world, a broader data definition would be ahead of time, and cover more situations, the opposite of a narrow data definition. On the other hand, a broad definition of the data would create an environment with opportunities for abusing positions from different stakeholders. For instance, the users of the IoT devices or related services may request access to all kinds of data generated, and that would result in a burden for the data holder (added costs and efforts).

The upside of a narrow (er) definition is that it's more specific, and it manages well the uncertainty among the stakeholders in the market and across different industries, on what kind and amount of data should be shared. It does not leave that much room for interpretation, hence there might be fewer claims in this regard. The downside would be that a narrow scope of data could probably mean no share of data at all in certain sectors. Nevertheless, a balance of the above would probably be a good solution as too broad or narrow a definition would neither make the market participants happy nor achieve the objectives set in the DA proposal.

2.4 With whom will the data be shared?

Chapter II of the DA proposal states that the data will be shared business to consumer, among business, business to research organizations, universities, etc. Furthermore, chapter V regulates the sharing of the data with public and EU institutions when there is an 'exceptional need' and certain conditions are met[23].

The purpose of sharing the data with consumers is to allow them to have more information on the product, to be able to make more informed decisions, switch between different providers, receive better aftermarket services, and purchase higher quality products, and with a more competitive price.[24]

As mentioned, the regulation will also enable the sharing of data under the ownership of the private sector (businesses) with public institutions/agencies (within the Union). Such data will only be shared if there are public emergencies (such as the Covid-19 pandemic or force majeure), to enable public bodies to react faster on behalf of public interest. The public body has to prove that there is an exceptional situation where it is needed to use specific data made

[23] EU Data Act Proposal, ch II and IV.

[24] Commission 'Data Act: Commission proposes measures for a fair and innovative data economy' (n 3).

available by the data holder. Nevertheless, even though there might be an exceptional need, the sharing of data will take place only if the needed data cannot be received from other sources in an effective and efficient way. The obligation to share the data with public authorities does apply to SMEs.[25] Public bodies may use the data shared with them only for the purpose that data was shared, not any other purposes.[26] Article 19 (2) states that public bodies may also require the sharing of trade secrets by the data holder if that is needed to achieve the goals for which the request for the share of the data was made.

Business-to-business data sharing will be done based on agreements that will be negotiated between businesses. The EU Commission will introduce model contractual clauses that will have a non-binding character, but that are expected to facilitate the negotiation.[27]

Article 5 and 6 of the DA proposal does not allow the users of IoT devices and third parties to share data with gatekeepers.[28] The EU Council and Parliament have not changed their position in the latest adopted version of the DA regarding the share of data with gatekeepers. They believe that the restriction for the sharing of data should stay in place, as initially proposed by the Commission and gatekeepers shall not be able to make data access claims.[29] As one of the objectives of the EU DA is to make sure there is a fair distribution of data in the EU market, it's considered essential that the restriction for sharing the data with the gatekeeper is in place. Nevertheless, in its adopted position, the EU Parliament has proposed adding language that clearly specifies that such restrictions do not prohibit the gatekeepers from obtaining the same data through other lawful means or directly from the manufacturers. The restriction applies only to the data from users or third parties.[30]

Kerber in his article expresses his concerns that allowing the manufacturer to share the data with the gatekeepers, gives the manufacturers of IoT devices exclusive the actual control over the data derived by an IoT device. Manufacturers can sell that data to the gatekeepers

[25] ibid.
[26] EU Data Act Proposal, art 19.
[27] ibid art 34.
[28] Council Regulation (EU) 2022/1925 of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 [2022] OJ L265/28. Arts 2(1) and 3(1) define 'Gatekeeper' as businesses that provide core platform services (in the area of online intermediation services, online search engines, cloud computing services, etc.) and have a significant influence in the market, their services are important not only for other businesses but also for users. An example of a Gatekeeper would be Amazon Web Services, Google, etc.
[29] Tom de Cordier and others, 'European Parliament and Council ready to start trilogue negotiations on EU Data Act - European Data law is getting closer' (*CMS Legal,* 29 March 2023) <https://news.cms.law/rv/ff00a7d1d0e3e1cf20dbf2caae4f85e46bbe647e> accessed 6 May 2023.
[30] Council of the EU, 'Interinstitutional Negotiations' (n 22) 10 ff.

as there are no limitations for manufacturers on that topic. Furthermore, they can also elect to produce, design, or create the IoT devices in a manner that includes technical features that give them more freedom and control over the data that is collected or can be collected from such a device. Such a position would give power to big tech companies to get control over the data which could lead to a certain data concentration in the future in the market.[31]

2.5 Conditions under which the data will be shared

The data holder or the manufacturer (when in the capacity of the data holder) provides and shares the data with the user, towards no financial compensation. In contrast, the data recipient can only access the data against reasonable compensation. In the case of small or medium size companies, the compensation should represent the actual costs incurred by the data holder to provide the data recipient with access to the data.[32] Such sharing of data should be done under the principles of fair, reasonable, and non-discriminatory. Furthermore, the Council, in its adopted position, suggests that when the agreement for a share of data B2B, the data holder shall provide the data under the same conditions to the same categories of data recipients unless the data holder has an objective explanation for different treatments of the same categories of data recipients.[33] Council has gone further by specifically defining what shall be included in the reasonable compensation and what the costs and margin that make a reasonable compensation are.[34]

In the case of public authorities, the DA proposal, Art. 20 (1) suggests that in the case of exceptional need, the data shall be shared with the data holder free of charge (no compensation involved). In the cases defined in Art. 15 (b) and (c) of the proposal, the data should be provided against a reasonable compensation that includes the costs incurred and a margin.[35] Council has suggested that the data shall be provided free of charge in the case of a public emergency and to mitigate a public emergency only if such a public body is not able to receive these data through other means in the same timely and effective way as could be offered by the data holder.[36] Furthermore, the data that will be obtained by public bodies, due to the exceptional need can further be shared with Research or non-profit organizations,

[31] Kerber (n 11) 129 ff.
[32] EU Data Act Proposal, art 9.
[33] Council of the EU, 'Interinstitutional Negotiations' (n 22) 21, para 41.
[34] ibid 21 ff, para 42 (a).
[35] EU Data Act Proposal, arts 15 and 20.
[36] Council of the EU, 'Interinstitutional Negotiations' (n 22) 56, art 15.

provided that these organizations will use the data for non-profit purposes or for public interest matters.[37]

2.6 Mechanisms for data sharing

The user has the right to use the data as they see it appropriate for lawful purposes. The user may decide to pass the data to third parties.[38] The system of data sharing with the consent of the user is based on the request of the user to the manufacturer or data holder. [39]

However, it is not clear what kind of contractual relationship will be established between the data holder, the user, and the data recipient when the user requests or consents to share the data with. In the adopted position of the Council, in recital 38, it's stated that the legislator has assumed that a contract is signed between the data holder and the third party.[40] Professor Wolfgang Kerber suggests that despite the user's intent to share the data with a data recipient, the user cannot directly share the data with such a party. A 'licensing agreement' could be signed (also confidentiality agreements when trade secrets are concerned) between the data holder and the recipient to fix the negotiated terms concerning data being and purposes data can be utilized.[41]

The Commission has included in the DA the development of model contractual terms to be used for data sharing. Such model contractual terms will not be mandatory but instead, an option to facilitate negotiating between businesses.[42] The European Law Institute (ELI) has also suggested these model clauses instead of standard contractual clauses similar to what is introduced for the sharing of personal data under the GDPR, as the second would introduce some default rules that could potentially contradict national laws.[43] Habich on the other hand points out that negotiations between the parties to reach an agreement would bring a lot of transaction costs, hence he sees the model clauses as a way to reduce such costs by having

[37] ibid 61, art 21.
[38] EU Data Act Proposal, paras 14 and 28.
[39] ibid art 18.
[40] Council of the EU, 'Interinstitutional Negotiations' (n 22) 20, para 38.
[41] Kerber (n 11) 122.
[42] EU Data Act Proposal, arts 34 and para 83.
[43] European Law Institute, 'ELI submits a response to the EU Commission's Public Consultations on the Data Act' (*European Law Institute,* 03 September 2023) 21-23 <https://europeanlawinstitute.eu/news-events/news-contd/news/eli-submits-a-response-to-the-european-commissions-public-consultation-on-the-data-act/> accessed 16 June 2023.

model classes and starting the negotiation process from there. Deviations can be included where necessary in order to save a lot of costs.[44]

In the EU DA, the EU Commission suggests adopting smart contracts as a tool for data sharing. Moreover, it sets specific standards to make smart contracts compliant and usable for the purpose. Some of the standards set for smart contracts include features to pause the execution of the contract if one of the parties requires so, be robust, safe, and provide access control. Nevertheless, many stakeholders in the area of smart contracts and blockchain disagree with this approach of the Commission arguing that it contradicts the foundations of smart contracts. Smart contracts from nature are designed to be self-executable contracts without the possibility to change/modify them.[45]

2.7 Switching between data processing service providers

As mentioned at the beginning of this chapter, one of the reasons for coming up with this legislative proposal was due to the high market share that non-EU cloud providers have in the EU. The approach of the Commission is to enable switching from one cloud provider to another one practically. In the impact study that the Commission did, some of the problems identified in the cloud market are the absence of common standard rules in reusing data, access of the governmental agencies in third countries (in some instances even without informing the EU user about such access and also unfair imbalances and negotiating power between cloud providers and EU businesses.[46]

Articles 23-26 of the DA proposal covers rules for switching of data processing service providers. The commission intends to remove obstacles concerning cloud provider switching, hence it suggests removing of commercial, contractual, and technical or organizational barriers from data processing services providers. Cloud providers must offer "transition support" whenever a customer wants to switch to a provider of the same services. Moreover, the cloud provider should not apply or apply certain charges for the switching process.[47]

---

[44] Erik Habich, 'FRAND Access to Data: Perspectives from the FRAND Licensing of Standard Essential Patents for the Data Act Proposal and the Digital Markets Act' (2022) 53 IIC, <https://ssrn.com/abstract=4119834> accessed 27 June 2023.

[45] Federico Casolari and others, 'How to Improve Smart Contracts in the European Union Data Act' (2023) 2 (9) *DISO* <https://doi.org/10.1007/s44206-023-00038-2> accessed 14 May 2023.

[46] Commission, 'Commission Staff Working Document - Impact Assessment Report' (n 7) 15-22.

[47] EU Data Act Proposal, art 23.

Council of Europe in its adopted position proposes to strengthen the measures for facilitating switching of cloud providers even further. It suggests that data processing services shall comply with the transparency principle and make available on their website the information about the jurisdiction that applies to the data and also what measures the provider has taken in order not to allow governmental agencies of third countries to have access to the data in contrary to the EU law.[48] The measures for switching between cloud providers will be subject to the final legislative negotiations.

[48] Council of the EU, 'Interinstitutional Negotiations' (n 22) 66, art 24 (a).

3 Stakeholder analysis

Stakeholders directly affected by the DA proposal are the consumers/users of IoT devices or related services (be it a natural person or a business), manufacturers of the IoT devices, businesses (in the capacity of the user, data recipient or data holder), third parties in the capacity of the data recipient (natural person or business entity) public institutions (member state or union institutions) and academic or research Institutions.

It should be noted that from the research, there is a big interest in the DA proposal from different stakeholders. Many have published position papers, stated their opinions, concerns, and recommended changes. Quite often these stakeholders have consulted the proposal with other stakeholders within the same industry/field and come up with joint statements.[49]

In the public consultation held by the EU Commission on DA, there was interest not only from EU MS stakeholders but also from the U.S.A, UK, Canada, Brazil, etc. The most participants were businesses (122 out of 449 which was the total of stakeholders). After the businesses, the biggest groups that showed interest were public authorities (100) and individuals (58).[50]

3.1 Position of businesses

From the public consultation that the Commission conducted, 91% of the companies that replied to this question admitted that they share data with other companies on a voluntary or mandatory basis. Nevertheless, they encounter issues concerning sharing of data. Among common issues are the lack of standards on formats (many different formats of the data), legal uncertainty, not being sure if the data will end in the hands of their competitors and dominating positions in contracting and negotiating.[51]

Furthermore, a significant reaction to the DA proposal comes also from 30 trade associations.[52] They believe the DA is being approved too early without first being tested in the market conditions. They claim there is a lot of uncertainty on the nature and amount of data required to be shared with users or data recipients and the legislator shall distinguish between the data to be shared with the consumer and the companies. Furthermore, there is a

[49] For example, European Business Association, the European Automobile Manufacturer's Association, Irelands' largest lobby group and business representatives (Ibec), etc.

[50] The public consultation took place in the form of a questionnaire sent to interested stakeholders.

[51] Commission, 'Public Consultation on the Data Act: Summary Report' (*EU Commission,* 06 December 2021). <https://digital-strategy.ec.europa.eu/en/library/public-consultation-data-act-summary-report> accessed 07 May 2023.

[52] Including Digital Europe, Business Europe and European Tech Alliance.

lot of uncertainty about the process of enforcing safeguards concerning trade secrets when the data will be made available to data recipients. Among the concerns of these business associations are also international data transfers as many companies operate in an international sphere and for those companies, data flows are critical to their operations.[53]

The European Automobile Manufacturers' Association (ACEA) states in its paper that they embrace the initiative and are already sharing the data with the users as per the DA proposal rules. Nevertheless, ACEA is concerned that some of the requirements proposed in the DA are 'unworkable'. ACEA believes that they do not serve the goal and to reach the objectives set for a data economy, instead, the opposite as they create a lot of uncertainty for businesses as these businesses will not know how the business-sensitive data will be safeguarded.[54]

In its position paper Digital, Online, Tech (DOT) Europe [55] has expressed four main concerns regarding DA. One of the concerns is related to data portability. DOT Europe supports the empowerment of users, by providing them access to the generated data. Still, it exposes businesses to the risk of trade secrets, intellectual property, negative consequences regarding competition, and privacy & security concerns (the users cannot protect the data like businesses). Furthermore, DOT Europe suggests that the restrictions for the user on sharing the data with Gatekeepers, should not be in place, arguing that there are already competition laws in place to make sure and safeguard that Gatekeepers comply with the rules of not abusing the dominant position they may have in the market. Another concern is related to the B2B data contracts. DOT Europe suggests that there is no need to provide model contract terms as Europe is a free market and businesses should be free to negotiate these terms independently. The third concern that DOT Europe has, is related to the access of public bodies to data. It states that the provisions provided in the DA proposal are too broad. Even though it has defined that the data should be shared only in the case of an "exceptional need" and there is no other alternative to obtain such data, DOT Europe suggests that the DA should shift the burden of proof to such a public body to prove the above. Regarding cloud switching, DOT Europe says that besides the confusion/unclarity, the rules are too ambitious and also beyond what is necessary to achieve the goal (in B2B). The last concern that DOT Europe

[53] Luca Bertuzzi, 'Industry associations ask EU policymakers to pull the breaks on Data Act' (*Euractiv,* 03 February 2023) <www.euractiv.com/section/digital/news/industry-associations-ask-eu-policymakers-to-pull-the-breaks-on-data-act/> accessed 08 May 2023.
[54] ACEA, 'Position paper - Proposal for a Data Act' (*ACEA,* 16 May 2022). <www.acea.auto/publication/position-paper-proposal-for-a-data-act/> accessed 9 May 2023.
[55] DOT Europe is an organization that represents the main internet companies. It has 23 members (as of May 19, 2023), among them are Apple, Google, Meta, Amazon, Microsoft, etc.

has expressed is related to international data transfers (non-personal data). DOT Europe states the restrictions set in Article 27 of the DA proposal, which are similar to the restrictions set for personal data regarding data transfers outside the EU, will discourage businesses from choosing global cloud providers as they may fear their compliance with DA. Furthermore, the sharing of non-personal data doesn't possess the same risks as sharing of personal data.[56]

Even after the latest political agreement reached between the EU Commission and Council on 28 June 2023, there is a lot of disappointment from businesses, especially about the final positions of these two institutions concerning trade secrets, cybersecurity, etc. [D]igital Europe believes that such a law will have negative consequences for the economy of Europe, and combined with other current issues (e.g., increase in energy prices), it will lead to a 'wave of de-industrialization' in Europe.[57]

3.2 Position of public institutions

In the public consultation held by the commission, 91% of the public authorities that participated in the public consultation stated that the sharing of data with public bodies legitimized under public interest is indeed needed and helpful. On the other hand, only 38% of business respondents think that public institutions should have access to the data produced or created by IoT devices or related services. The respondents identified an issue about data sharing with public institutions the lack of legal information in this area, no incentives to share the data, and that there is uncertainty if the data shared will solely be used for the purpose it was shared.[58] EDPS and EDPB have raised issues on compliance with the DA regarding protecting personal data.[59]

3.3 Consumers

Except for the participation (58 citizens out of 449 stakeholders) in the initial public consultation held by the Commission, the author did not notice any other direct opinion or position of the citizens concerning the DA proposal. Nevertheless, the opinion of the individuals cannot specifically be extracted.[60]

---

[56] DOT Europe, 'DOT Europe publishes position paper on Data Act' (*DOT Europe,* 04 May 2022). <https://doteurope.eu/news/dot-europe-publishes-position-paper-on-data-act/> accessed 21 May 2023.

[57] Digital Europe, 'Data Act agreement: The necessary balance is yet to be achieved' (*DIGITALEUROPE,* 28 June 2023) <https://www.digitaleurope.org/news/data-act-agreement-the-necessary-balance-is-yet-to-be-achieved> accessed 29 July 2023.

[58] Commission, 'Public Consultation on the Data Act: Summary Report' (n 51).

[59] See detailed information about the report is in chapter 4, section 2.

[60] Commission, 'Public Consultation on the Data Act: Summary Report' (n 51).

However, there is a press release from the European Consumer Organization (BEUC) that states its position on the DA proposal advocating for consumer rights. BEUC believes that since the consumer is the originator of the data and the consumer helps in creating such data (with their device), the consumer should have a controlling position in deciding with whom the data can be shared. Furthermore, BEUC states that the DA should enable the consumer to share the data generated by a device with a competitor of such device if the consumer elects to do so. BEUC suggests a consumer-centric position concerning data sharing.[61]

Insurance Europe has stated a similar position in responding to the EC consultation on the DA proposal. It welcomes the initiative, but it suggests that the consumers should give their consent with whom the data should be shared, and such consent shall be given in a simple, straightforward, and verifiable way.[62]

3.4 Position of research & non-profit organizations

Max Planck Institute supports the initiative of the Commission and the fact that it's proposed in the form of horizontal legislation. Yet, it suggests that sector-effective rules would be more effective in this regard, than having the future legislation to align with the DA proposal. Furthermore, the Max Planck Institute criticizes the proposal for not covering all relevant points to reach the objectives set (e.g., take into consideration the recent developments in artificial intelligence (AI). It believes that the current proposal might be a bit too far-reaching and not define the right tools to fulfill the objectives set, hence the EU should narrow the scope of application of the DA proposal. Since the law is a horizontal legislation (not a directive), Max Planck Institute is concerned that due to unclear text, this legislation will create uncertainty during the implementation and will cause MS not to have harmonized rules, therefore undermining its effectiveness.[63]

Universities see the DA proposal as a missed opportunity for them to benefit from the access to data for their research. Even though research institutions are set to benefit from the DA,

[61] BEUC, 'Data Act important for competition and consumer choice' (*BEUC,* 23 February 2022) <https://www.beuc.eu/press-releases/data-act-important-competition-and-consumer-choice> accessed 9 May 2023.

[62] Insurance Europe, 'Response to EC consultation on Data Act proposal' (*Insurance Europe,* 17 May 2022) <https://www.insuranceeurope.eu/publications/2606/response-to-ec-consultation-on-data-act-proposal/> accessed 10 May 2023.

[63] Josef Drexl and others 'Position Statement of the Max Planck Institute for Innovation and Competition of 25 May 2022 on the Commission's Proposal of 23 February 2022 for a Regulation on Harmonised Rules on Fair Access to and Use of Data (Data Act)' (2022) Max Planck Institute for Innovation and Competition Research Paper 22-05, 3-5 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4136484> accessed 08 May 2023.

it's not clear how and can they benefit exactly. [64] The MS are trying to include rules in the DA proposal regarding research. They want the research rules in the DA proposal to align with the national research rules set in the existing national laws. Universities seem to be satisfied with the proposed changes in the latest version of the DA proposal, even though the DA overall does give the impression of not taking that carefully into consideration the use of data for research purposes.[65]

3.5 Charity organizations

Except for the position papers of the non-profit organizations that conduct research activities as mentioned above (Max Planck Institute, ELI, etc.) the author could not find any position papers to DA proposals from any charity organization.

3.6 Stakeholder analysis matrix

As analyzed above, one of the goals of the DA proposal is to strike a balance between stakeholders due to the fact that some stakeholders have more access to and benefit from data generated than other stakeholders. In the position papers, different stakeholders have different concerns. The chart below highlights some of the main concerns of the stakeholders (identified in this chapter, see above), and provides an overview of where each stakeholder stands for which issue, and is followed by an analysis on whether there can be formed any collaborations between different stakeholder for different concerns, or not.

[64] Goda Naujokaitytė, 'EU is poised to give industry a data boost – and universities want in' (*Science Business,* 14 March 2023). <https://sciencebusiness.net/news/Data/eu-poised-give-industry-data-boost-and-universities-want> accessed 14 May 2023.

[65] Goda Naujokaitytė, 'EU Data Act is causing friction' (*Science Business,* 11 May 2023) <https://sciencebusiness.net/news/eu-data-act-causing-friction> accessed 21 June 2023.

Categories	**Users (businesses and consumers)** e.g. users of vehicles, machines, etc.	**Data holders** (manufacturer of IoT devices/related services)	**Data recipients** (businesses that receive data - e.g. for aftermarket services)	**Data processing service providers** (e.g. Amazon Web Services, Google Cloud)	**Public institutions** (MS or Union Institutions)	**Research and non-profit institutions** (e.g. Max Planck Institution)	**EU Legislator** (e.g. EU Commission)
Interested in data sharing	Yes, they want access to data generated by their IoT device	In principle they support the concept of DA, but they think it will also be a burden for them due to compliance (design of the IoT device)	Yes, they are interested in receiving data	In principle they support the concept. Nevertheless they require to distinguish between different services in this area (e.g. SaaS with PaaS)	Yes, they support the data sharing and have interest in it	Yes, the research and non for profit org. find the DA a good initiative and they expect to benefit from data sharing	Yes, this is considered a very important initiative
IP and Trade Secrets concerns	Businesess in the quality of users are not affected	Yes, businesses in the quality of data holders are one of the most concerned parties about this topic	As long as the data recipients only receive data, they are not directly affected from the share of trade secrets	Yes, they are concerned about IP and trade secrets disclosure	There doesn't seem to be any comments in this topic	Yes, they argue that there is a high risk for IP and trade secret holders	Claims that have taken it into consideration the risk and have put in place measures to prevent unauthorised disclosure or misuse
Competition concerns	Businesses seem to benefit, they will receive more data and will be able to compete against bigger players in the market. Users might get better prices and products	Yes, they are the most concerned party in this regard	No, there are no concerns. It's actually the opposite, they will be empowered and able to strengthen their position in the market	Yes, they are concerned as businesses will be able to switch providers easier than before	No concerns are expressed in this regard	They think the DA will have a negative effect on competition	Claims that have taken it into consideration and no risk identified
Personal data concerns	No statement has been found, but it can be implied that consumers and businesses want personal data handled in compliance with GDPR	Yes, because they might be fined for non-compliance if the data is not being handled in compliance with the GDPR rules	Yes, because they might be fined for non-compliance if the data is not being handled in compliance with the GDPR rules	Not directly affected from but instead tasked to offer support for transferring data to another provider	No concerns are expressed in this regard. Presumably there might be some concerns	Yes, they are concerned as they think there are issues and confusion with the current setting	The leigslator states that all personal data will be handled as per the GDPR
Uncertainty on the nature and amount of data to be shared	Yes, it's not clear what data can/should be generated by an IoT device or related service	Yes, it's not clear what data should be generated by an IoT device or related service and shared with the user and data recipient	Yes, it's not clear what data can/should be generated by an IoT device or related service	Not directly affected from but instead tasked to offer support for transferring data to another provider	No concerns are expressed in this regard. Presumably they might be concerned	Yes, they claim that the legislator has not clearly defined this and the provided definition is too broad	EP, Commission and Council they are trying to address this topic better in their negotiations
Want more control over the data	Yes, want to have control over the data and the right to decide on the data generated by them	Yes, they want to be in control of the data generated by the IoT device or related service produced by them	Yes, they want as much access as possible so they can better provide the user with products/services	They want more control over the process	No opinion made available in this matter	Think that the data holder has actually control over the data, hence more bargaining power	Trying to strike a balance between stakeholders

One of the areas of compromise could be IP and trade secret concerns as many stakeholders are business (or stakeholders that support/want to accommodate businesses), and they can understand the risk that it comes from the disclosure of trade secrets. As for consumers (natural persons), as long as they receive the data they need, they should be fine, as long as data holders don't refuse to provide data on these grounds. Nevertheless, there should also be a commitment and trust formation from businesses in the quality of data holders so that they won't misuse this part.

Personal data concerns are also another matter where most stakeholders would agree that the risk of unlawful personal data processing should be minimized/mitigated. Consumers want their personal data to be handled in compliance with GDPR, and so want businesses, otherwise, they will receive fines for non-compliance. Public institutions would want the citizens of their countries to feel that their personal data rights are being safeguarded

properly. However, the processes defined so far need to be cross-checked with GDPR compliance.

Another area where there could be a consensus between the parties is about the amount and the nature of data to be shared. It seems that ambiguities in this matter are a cause of concern for all stakeholders as once the Data Act enters into force, all stakeholders will be faced with this issue. As mentioned in this paper, the legislator is also trying to clarify this subject better. However, it will be difficult to agree on what amount of data to share because every data holder produces/trades different devices and the nature and amount of data could be different for each industry.

The matter of control over data might be a difficult topic to negotiate as different stakeholders want more control over the data. As mentioned at the beginning of this subchapter, as the purpose of this law is to strike a balance between the power held by different stakeholders, it could be presumed that no overall agreement would be reached on this matter, but rather a coalition between stakeholders (e.g., research institution/non-profit, users and legislator and on the other side data holder and data processing service providers).

4 Problems identified in the Data Act

4.1 Concerns regarding trade secrets & other intellectual property rights

Article 4 of the DA proposal states that 'Trade secrets shall only be disclosed provided that all specific necessary measures are taken to preserve the confidentiality of trade secrets especially with respect to third parties.'[66] Article 5 (8) allows disclosing trade secrets to third parties[67] solely to the extent needed to fulfill the purpose agreed between the parties and only if there are measures in place to ensure the protection of trade secrets.

As stated in the provisions above, the DA proposal requires disclosure of trade secrets, provided that there are measures in place to safeguard the confidentiality of such proprietary information. Many businesses and business associations have expressed their concerns regarding the provisions of the trade secrets in the proposal. In a joint statement, 30 organizations refer to the DA proposal as a 'leap into the unknown' and recommend that the EU makes sure that there is adequate protection of trade secrets, and that all the necessary safeguards to guarantee the appropriate utilization of data and no unfair competition is involved.[68] According to BusinessEurope and Orgalim associations,[69] current provisions on the trade secrets and the amendments suggested in the DA proposal entail a potential risk to future innovation in the European Union and that might have negative consequences on the business after the implementation of the act.[70]

In the study conducted by the EU Commission about safeguarding of trade secrets, one of the main findings in this topic was that EU businesses are not prepared or do not have mature expertise regarding the protection of trade secrets provided through sharing of the data. The authors suggest that the reasons for the lack of expertise in this area may be that data-sharing methods are still at an early stage, also the Trade Secrets Directive (EU) 2016/943 (TSD)

[66] Commission, 'Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)' COM (2022) 68 final (EU Data Act Proposal), art 4.
[67] Article 2 (7) of the Data Act Proposal provides a definition of the data recipient and clarifies that third parties are the recipients of the data following the user's request.
[68] Francesco Guerzoni, Digital Transformation: Joint Statement - The Data Act is a leap into the unknown' (*Oraglim,* 1 February 2023), <https://orgalim.eu/position-papers/digital-transformation-joint-statement-data-act-leap-unknown> accessed 14 March 2023.
[69] In the position statement issued by them (see full reference on footnote 70 below), they present themselves as one of the biggest associations in the tech industry, and state that they represent a significant number of European businesses in this industry.
[70] Francesco Guerzoni, 'Digital Transformation: Underestimating the Data Act's impact on trade secrets' protection will undermine European industrial competitiveness' (*Oraglim,* 17 January 2023) <https://orgalim.eu/position-papers/digital-transformation-underestimating-data-acts-impact-trade-secrets-protection> accessed 14 March 2023.

was introduced in recent years, hence companies have not gained enough experience yet. Furthermore, in many companies, there are no specialized teams for this topic, but instead are handled by different teams, such as IT, IP, etc. There is also a lot of uncertainty about the qualities that certain data should have to obtain trade secret protection. According to the study, the answer to whether the protection of trade secrets makes it easier to share data, or not, is not fixed, as there might be circumstances when it does facilitate data sharing, and also cases when it doesn't due to uncertainties that parties have (as mentioned above in this paragraph), concerns that the trade secret holder may actually cede control of such data, and the fact that there are no encouragement or motivation for sharing of a such data (e.g. benefits, remuneration, etc.).[71]

ACEA suggests that the power of deciding whether the share of a trade secret is strictly necessary should be vested with the trade secret holder. Furthermore, when a public body requests the share of a trade secret, the consent of the trade secret holder should be taken, and safeguards should be in place with the public institutions to ensure that such trade secrets are kept confidential.[72]

The Council has proposed in its adopted position additional measures to address the concerns of potentially affected businesses. Council proposes stricter language concerning the protection of trade secrets. Trade secrets shall only be shared after the user, or the data recipient consented by the user has demonstrated that the essential technical measures to ensure the protection of such data are in place. The trade secrets shared can only be used by the data recipient solely for the agreed-upon goals with and consented to by the user, and not more data than needed to fulfill such purposes. Suppose the data holder believes the measures in place are not enough to ensure such confidentiality, the data holder has the burden of proof to show that such measures are not enough and to ask further the user or the third party to adopt additional measures of a technical and organizational character Furthermore, if the data holder refuses to share data, by claiming that the data holder would incur damages if such share of trade secrets takes place, the data holder again has the burden

[71] European Commission, European Innovation Council and SMEs Executive Agency, 'Study on the legal protection of trade secrets in the context of the data economy – Final report' (*Publications Office of the European Union,* 2020) 2-3 <https://data.europa.eu/doi/10.2826/021443> accessed 3 June 2023.
[72] ACEA, 'Position paper - Proposal for a Data Act' (*ACEA,* 16 May 2022). <www.acea.auto/publication/position-paper-proposal-for-a-data-act/> accessed 9 May 2023.

of proof and additionally shall inform the authority in charge of the supervision of issues arising from this proposal (following Article 31 of the DA proposal).[73]

BusinessEurope and Oraglim[74] state that although there are proposed changes to the initial DA Proposal, these changes still do not provide enough safeguards to protect trade secrets. Introducing confidentiality agreements is not enough. These associations call not to lower the level of protection that is set in the Trade Secrets Directive 2016/943. Furthermore, they claim that assessing the situation only after two years after the implementation of this legislation, to see what effects it has had on this topic, would cause damage to the businesses in the EU market and that such damages would put Europe behind in this area and bring negative consequences in the single market.[75]

In its impact assessment, the EU Commission has also identified this issue and that the violation of trade secrets could lead companies to make fewer investments and be less innovative, especially SMEs. Nevertheless, it highlights that the risks are mitigated by including the unfairness test concerning data-sharing contracts which will be able to make up for the negotiation power of the weaker party in the transaction. Moreover, the EU Commission also recognizes the risk of disclosing trade secrets from data access rights to not only free riders but also to big global companies. It states that such risks are mitigated by the provision of the DA proposal, and the freedom of the manufacturers to share the data with whom they agree, in the quality of the data holder they will also get compensation when requested to share the data with third parties and take action if such data will be used for unlawful purposes. The Commission also suggests that the use of tools like smart contracts will boost the security of data.[76]

Another approach, in support of the Commission's reasoning, is that while it is important to protect trade secrets (not to destroy the secrecy), it's also important that data holders do not hide or reject sharing data with users, or third parties based on the vague requirements of

[73] Council of the EU, '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) - Mandate for negotiations with the European Parliament' (Interinstitutional Negotiations) (2023) 7413/23, 46ff <https://data.consilium.europa.eu/doc/document/ST-7413-2023-INIT/en/pdf> accessed 16 May 2023.

[74] BusinessEurope and Oraglim refer to themselves as among the largest Technology industries associations in Europe.

[75] Guerzoni, 'Underestimating the Data Act's impact on trade secrets' protection will undermine European industrial competitiveness' (n 70).

[76] Commission, 'Accompanying Commission Staff Working Document - Impact Assessment Report', SWD (2022) 34 final, 145-146 <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022SC0034&from=EN> accessed 4 February 2023.

trade secrets (what qualifies as a trade secret and what not). Centre on Regulation in Europe (CERRE) considers the requirement of having confidentiality agreements in place and appropriate protection measures as a good balance for the disclosure of trade secrets. Moreover, CERRE sees Article 8 (6) of the DA proposal as an issue as it allows data holders not to disclose trade secrets if such disclosure falls within the meaning of TSD.[77]

However, it is not clear if such confidentiality obligations refer to the confidential business information of the data holder or also of third parties. Picht raises the question of whether it is fair, or not that the user and the third party with a contract between them oblige the data holder to reveal its trade secrets. Picht suggests that the legislator has failed to provide clarity on this important topic.[78]

4.2 Problems arising from personal data and mixed data sets

Article 1 (3) and (4) of the DA proposal specify that if any personal data should be processed concerning the data sharing obligations, it should be done in compliance with the e-Privacy Directive and GDPR. The measures set in the proposed DA should act as complementary to those set in the GDPR and the e-Privacy Directive.[79] Nevertheless, the text in the proposed draft is not very clear, hence it has created some tension in the personal data protection sphere. It has drawn the attention of the European Data Protection Board (EDPB) and European Data Protection Supervisor (EDPS), which with a joint opinion expressed their concerns concerning the protection of personal data.[80] There are the following significant concerns about the provisions set in the DA proposal that undermine the existing obligations under GDPR and e-Privacy directive:

First, the proposal is written using a language that does not specify which law shall prevail in case there is a conflict in the implementation of the DA provisions. Different from the Data Governance Act, which clearly has specified that the GDPR should prevail, in the case

[77] Giuseppe Colangelo, 'European Proposal for Data Act - A First Assessment' (2022) Centre on Regulation in Europe Evaluation Paper, 20-21 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4199565> accessed 04 June 2023.

[78] Peter Georg Picht, 'Caught in the Acts: Framing mandatory data access transactions under the Data Act, further EU digital regulations acts and competition law' (2022) Max Planck Institute for Innovation & Competition Research Paper 22-12, 38 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4076842> accessed 13 June 2023.

[79] EU Data Act Proposal, art 1 (2) (4).

[80] EDPB, EDPS, 'Joint Opinion 02/2022 on the Proposal of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)' (*EDPS,* 4 May 2022) 2 <https://edps.europa.eu/system/files/2022-05/22-05-05_edps-edpb-jo-data-act_en.pdf> accessed 13 March 2023.

of the DA, that has not been answered and it is still an open question.[81] EDPB and EDPS ask the legislator to specify that laws on data protection have priority when processing personal data. EDPB and EDPS suggest limiting the processing of personal data to a minimum and that the devices should be produced/used in a manner that allows anonymization of data, without prejudice to the title or ownership rights.

Second, there is apprehension regarding processing of personal data related to users who may have access to the data generated by an IoT device. It could be that the user has the same interest in the personal data as does the manufacturer of the device and both want to make use of the data generated by using a device. The problem that arises from such use of data by the user is that the user may not necessarily be the data subject[82] and the user is a party in possession of data with an interest in making use of the data interest which may or may not be aligned with the interest of the data subject.[83] EDPB and EDPS emphasize the need for restrictions and limitations on using personal data created or derived from the use of a IoT device or service connected to such a device, by someone other than the data subject. They suggest that personal data is handled only as per the applicable privacy laws and that any further processing of the data is communicated accordingly to the affected data subject (s). In any case, the processing can only take place under the rules and restrictions set in Articles 6 and 9 of the GDPR, and the rules set in Article 5 (3) of the ePrivacy Directive.[84]

By processing the information generated by IoT and IoB, sensitive information related to individuals' private lives (e.g., vehicles, health devices, etc.), would create vulnerability.[85] Marc Rotenberg, also suggests techniques to anonymize personal data, to aggregate them. Such de-identification techniques should be rebooted, the liability should be assigned to the party responsible to ensure the anonymization of data (de-identify them) to comply with GDPR.[86]

---

[81] Marc Rotenberg, 'ELI Webinar on the Data Act: How to Boost the European Data Economy?' (*European Law Institute,* 24 May 2022) (Webinar) <https://europeanlawinstitute.eu/news-events/upcoming-events/events-sync/news/eli-webinar-on-the-data-act-how-to-boost-the-european-data-economy-2/?tx_news_pi1%5Bcontroller%5D=News&tx_news_pi1%5Baction%5D=detail&cHash=3f711f21c32dc495d4cc864440b66a75> accessed 16 May 2023.

[82] Data subject as per GDPR is the owner of the personal data (natural person).

[83] Marc Rotenberg, 'ELI Webinar on the Data Act: How to Boost the European Data Economy?' (n 81).

[84] EDPB, EDPS (n 80) 3.

[85] Ibid 8.

[86] Marc Rotenberg, 'ELI Webinar on the Data Act: How to Boost the European Data Economy?' (n 81).

Third, under the DA, there is the provision of sharing data with the Union's public institutions or agencies in case of exceptional circumstances.[87] Such use of personal data may not align with the protection under GDPR. EDPS and EDPB are concerned that allowing public institutions to process personal data may contradict the data subject's interest and it is uncertain if in practice the data will be shared in proportion with the importance of the request and only when it's necessary. EDPS and EDPB suggest that the circumstances when processing personal data under the DA proposal are not clearly defined and that, from time to time, might lead to unlawful processing of personal data.[88]

The *fourth* issue is related to Chapter IX of the proposal. DA proposal, specifically Article 31 states that each MS should define one or more competent authorities to monitor compliance with the DA. Even though it is defined that when it comes to matters that personal data is involved, it is the responsibility of the privacy authorities to deal with the issue, EDPS, and EDPB explain that it is unclear how the concerned parties (user, data holder, etc.) will be able to define from the start if personal data is involved or not, hence confusion on where to lodge a complaint may occur from time to time. There might also be overlapping of the tasks for both authorities and if there is poor coordination that might lead to negative consequences, such as handling and processing of personal data in breach of GDPR. Furthermore, EDPS & EDPB suggest changes in the act, in the cases when mixed data sets (personal and non-personal data cannot be separated/split), by defining that the role of personal data supervisory authorities should take precedence in case of discrepancies between data protection authorities and the designated authority for the DA compliance.[89]

Moreover, Digital Europe says that such general provisions on the regime of the mixed data sets will open the door to different interpretations from various implementation authorities, hence increasing the legal uncertainty for companies. Digital Europe says such issues shall be remedied, otherwise, it will lead to unlawful processing of personal data as the data subjects might not have consented to the specific processing scenario. It recommends that competent authorities examine/analyze a few scenarios where mixed data sets may be involved and such issues are to be addressed to the DPA. The competent authority on the

[87] EU Data Act Proposal, ch V.
[88] EDPB, EDPS (n 80) 3.
[89] Ibid 25-27.

EU level responsible for the application of DA, shall collaborate with EDPB and issue joint instructions to facilitate the work for data holders and all involved parties in data sharing.[90]

4.3 Can the data shared under the provisions of the Data Act be used for training AI purposes?

Prior to the publication of the DA proposal, there were hopes that the DA would regulate access to the data for training AI models. Mauritz Kop, in his paper, expresses the upcoming DA as a tremendous opportunity for the purposes of processing the data for machine learning purposes. He indeed saw this upcoming proposal as the one that would remove all regulatory obstacles in this regard and finally make use of data within the EU for machine learning purposes. Furthermore, in his paper, he went further and identified some of the problems that might arise in this topic and proposed solutions to the identified problems. Kop identities as significant issues in using data for machine learning, GDPR, IP, and property ownership. He suggests that to make AI thrive and not create any potential conflict with the IP and GDPR, the data should be cleared of any IP rights (e.g., cleared of books, photos, or any other copyright rights, before being reproduced by AI) before feeding it to AI models for training. Trade secrets should be kept in the contracts and the Trade Secrets Directive shall be revised, where the definition of trade secrets shall be narrowed down.[91]

Moreover, it seems like the EU was planning or investigating the idea of regulating this area, as in the questionnaire sent by the EU Commission for public consultation, from the business representatives, there was a question related to that. 29 % of the respondents (businesses) that answered this question, confirmed that they use data for training algorithms for AI.[92]

According to the Max Planck Institute's position, even though the Commission states that it has taken into consideration all the technological developments in the data economy, such as cloud computing and artificial intelligence, however, it has not explicitly stated nor analyzed in the DA proposal whether or not the data that will be shared can be used for the training of AI. As Max Planck Institute suggests, it would need another piece of legislation

[90] Digital Europe, 'Rebalancing the Data Act' (*DIGITALEUROPE*, 01 September 2022) 27ff <https://www.digitaleurope.org/resources/rebalancing-the-data-act/> accessed 25 May 2023.
[91] Mauritz Kop, 'The Right to Process Data for Machine Learning Purposes in the EU' (*Standord Law School,* November 2020) 3ff <https://law.stanford.edu/wp-content/uploads/2020/11/Mauritz-Kop_The-Right-to-Process-Data-for-Machine-Learning-Purposes-in-the-EU.pdf> accessed 14 June 2023.
[92] Commission, 'Public Consultation on the Data Act: Summary Report' (*EU Commission,* 06 December 2021) <https://digital-strategy.ec.europa.eu/en/library/public-consultation-data-act-summary-report> accessed 07 May 2023.

at a later point to regulate this area and provide details on how the data processing for machine learning purposes shall take place.[93]

4.4 Too much power for the manufacturer of the IoT device and related services?

When reading the DA proposal, it's unclear whose interests the EU is trying to address. At first glance, the proposal seems to be user centric. Specific stakeholders claim that it sides with the user by giving the user too much power, and other stakeholders think that the data holder (manufacturer) is empowered more.

ACEA argues that the obligation of the manufacturers to design and manufacture the product in a way that makes the data accessible for the user is burdensome for the manufacturers. First, the law shall clearly specify what data shall be shared with the users as without a clear definition of what data can be shared with the user, the manufacturers cannot fully understand and comply with their obligations set in the DA proposal. Furthermore, ACEA suggests that the primary duty of a manufacturer is to design the product in a way that fulfills the function it was created for, not to share data. Being forced to design the product in a way that generates specific data, would lead to additional costs for manufacturers, costs which would have to be reflected in the price of the product.[94]

Vodafone (representing itself as one of the leaders of IoT devices), recommends changes to Article 3 (1) of the DA proposal. It proposes adding the language that states the manufacturers should design the product in a way that allows access to data 'where possible and feasible' and limited only to the data that the user has directly contributed to generating.[95]

The adopted position from the Parliament, suggests changes to Article 3 (1) of the DA proposal. Such changes state that the manufacturers of the connected products shall design

---

[93] Josef Drexl and others 'Position Statement of the Max Planck Institute for Innovation and Competition of 25 May 2022 on the Commission's Proposal of 23 February 2022 for a Regulation on Harmonised Rules on Fair Access to and Use of Data (Data Act)' (2022) Max Planck Institute for Innovation and Competition Research Paper 22-05, 4-5 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4136484> accessed 08 May 2023.

[94] ACEA, 'Position paper - Proposal for a Data Act' (n 72) 4-5.

[95] Irish Department of Enterprise, Trade and Employment, 'Call for views in response to the European Commission's public consultation on the Data Act' (*Enterprise GOV,* 1 April 2022) <https://enterprise.gov.ie/en/consultations/call-for-views-in-response-to-european-commission-public-consultation-on-the-data-act.html>, Vodafone Position Paper on EU Data Act <https://enterprise.gov.ie/en/consultations/consultations-files/vodafone-submission-data-act-consultation.pdf> accessed 10 May 2023.

the product in a way that allows collecting and generating the data with very little effort making the data available and usable format for the user or the third party.[96]

Kerber on the other hand suggests that even though the DA proposal intends to balance these rights, it's actually showing the opposite. It might have helped to strengthen the 'de facto' power in the hands of data holders (manufacturers) of the IoT devices. He suggests that the manufacturers decide what data can be made available to the users. Furthermore, there is no incentive for the manufacturers to make available the data to the user.[97] Drexl (et al.) also support the argument that the proposal gives the manufacturers exclusive control over the data. They design the product in a way that also doesn't support the aftermarket services and, in some instances, when the vendor has quite some power, it may create the vendor lock-in. Due to the position of the suppliers, they can technically prevent the information from their buyers and be able to control the after-service market. Moreover, the DA has only thought about the data dependency of the user, downstream data dependent, not upstream data dependency. This makes the suppliers of component parts dependent on the manufacturer; hence the development of such services depends on the manufacturer.[98]

The power of the user can be extracted from the fact that the user is the one who decides with whom to share the data. As stated herein, the user is the owner of the data and the data holder has a license to use the data.[99] Furthermore, there is no limit for users on the purposes of using the data they receive from the data holder, except for protecting trade secrets and the restriction to not develop a product similar to the one the manufacturer is offering.

How easy is it to decide what non-personal data is/should be generated by the IoT device? It appears that this is a very complicated topic that differs from one industry to the other. It is also not clear what data can/shall be collected and shared with the user. The likelihood is that the data holder (manufacturer) will decide on that and practically have the power to

[96] European Parliament, 'Amendments adopted by the European Parliament on March 2023 on the proposal for a regulation of the European Parliament and of the Council in harmonsed rules on fair access to and use of data (Data Act) (COM(2022)0068 – C9-0051/2022 – 2022/0047(COD))' (Amendments by the European Parliament to the Commission proposal) <https://www.europarl.europa.eu/doceo/document/TA-9-2023-0069_EN.pdf> accessed 24 July 2024.
[97] Wolfgang Kerber, 'Governance of IoT Data: Why the EU Data Act will not fulfill its objectives' (2023) 72 (2) GRUR International, 122 <https://doi.org/10.1093/grurint/ikac107> accessed 29 April 2023.
[98] Drexl and others (n 93) 15-18.
[99] Kerber (n 97) 123.

generate such data until there is further detailed guidance, sector-specific, or examples from dispute resolution where the court or DSBs under the DA decide on certain cases.

4.5 Switching between data processing services

As mentioned in section 2.7 of this paper, one of the objectives of the DA is also to facilitate the switching between various cloud providers. However, the rules on cloud switching were criticized initially when included in the DA proposal, and specific issues were identified. However, up to the current legislative phase the primary obligations identified in the initial proposal are still upheld, but clarification language is included. Council, in its adopted version, explains that changes are included in the text, to provide more precise and wider rules for effective cloud switching and add that the security of data should be maintained during the switching process.[100]

One of the concerns that DOT Europe brings is that the DA proposal doesn't distinguish between different data processing services, such as infrastructure-level services, software services, etc. According to DOT Europe, such services are not always interchangeable, and asking providers to remove obstacles and giving 30-day deadlines (which can be extended up to 6 months), is very complicated and not always possible. Sometimes the obstacle may be of a technical nature and unable to be removed, or it might be the responsibility of the new provider to take specific actions. Moreover, they claim that having mandatory technical specifications does not serve to incentivize innovation among providers. Lastly, DOT Europe proposes a transparent pricing structure for the support that they will provide concerning switching providers, by considering it an appropriate thing to do.[101]

The above argument is also partially supported by Digital Europe. Digital Europe also suggests that the proposal should take into consideration different cloud services (IaaS, SaaS, PaaS, etc.), the complexity and the volume of data stored in these clouds, and the responsibilities between the cloud providers and Customers shall be clearly defined.[102]

Some critics believe that the EU is using the pretext of European trade secrets being disclosed to U.S. intelligence agencies to discriminate against U.S. cloud providers, due to the cloud services in Europe. Such belief is based on the efforts of the EU to create its cloud

[100] Council of the EU, 'Interinstitutional Negotiations' (n 73) 4.
[101] DOT Europe, 'DOT Europe publishes position paper on Data Act' (*DOT Europe,* 04 May 2022). <https://doteurope.eu/news/dot-europe-publishes-position-paper-on-data-act/> accessed 21 May 2023.
[102] Digital Europe, 'Rebalancing the Data Act' (n 90).

framework GAIA-X (the European Cloud Platform) and to develop its domestic technology industry. The authors believe that it would cost Europe billions to establish its own data centers (by European cloud providers) and that the most feasible solution would be to develop the internal technology with U.S. providers as this is also needed for EU companies to stay competitive in the U.S. market.[103]

4.6 International data transfers

Chapter VII of the DA in the adopted version from the Council, covers unlawful non-personal data transfer to third countries in the context of providing data processing services. It forbids sharing non-personal data with governmental agencies of third countries, where such transfer would contradict EU law or the law of any MS. The whole chapter has only article 27 which covers the rules for international non-personal data transfers. Council, in its adopted position, has clarified the title of the article to limit it to governmental access only.[104]

Digital Europe compares the data transfer regime set in article 27 of the DA proposes a regime for personal data transfer and suggests that applying a similar regime for non-personal data would bring a lot of uncertainty for businesses that operate internationally. They suggest that Article 27 should be deleted entirely.[105]

Max Planck Institute refers to Article 27 of the DA proposal as 'perhaps the most problematic chapter of the proposal'.[106] Max Planck also points out that the data sharing regime in Article 27 is very similar to the one in the GDPR, which the EU later introduced in the DGA and now is included in the DA. The authors explain that the reason why it was included in the GDPR, is due to sensitive character and concerns about personal data as a fundamental right, and the level of protection it requires. Applying the same concept to the DA means acting against the objectives set in the act, promoting data sharing and cross-border cooperation with regards to data sharing.[107]

---

[103] Alexander Wirth, Giovanni Tricco and Maricaremen Martinez, 'Clouds on the Horizon: Europe's Cloud Policy threatens transatlantic digital harmony' (*CEPA,* 10 May 2022) <https://cepa.org/article/clouds-on-the-horizon-europes-cloud-policy-threatens-transatlantic-digital-harmony/> accessed 14 June 2023.

[104] EU Data Act Proposal, art 27.

[105] Digital Europe, 'Rebalancing the Data Act' (n 90).

[106] Drexl and others (n 93) 69-70

[107] Ibid.

Articles 27 (2) and (3) refer to the situations where the data service providers receive a request (be it an administrative request or a judgment), from a governmental agency/court of a third country, to share the data that the provider keeps within the EU. Article 27(2) regulates the cases where there is already an international agreement between the MS/EU and the third country, and what is to be done by the data processing provider is clear, as the decision will be enforced as per the international agreement between the parties. The situation in the case of Article 27 (3) it's not clear though, as it defines the procedure to be followed in case there is no international agreement or treaty between the EU or the MS and the third country. In such situations, the data processing provider will self-assess if the criteria set in the provision are met or not, or ask the competent authority to do such evaluation. It is however not clear which is the competent authority to decide about the matter, as the reference is not the same as in article 10 or 31 of the DA proposal. The Max Planck Institute suggests that the solution meant by the EU Commission for such matters could be solved as per private law (start litigation before the competent court). Nevertheless, current conflicts with private law should be removed from the text of the proposal.[108]

Moreover, ACEA considers the requirements set in 27(3) as "unworkable" and states that a private entity cannot take a judicial role and assess the situation every time there is a request for data access. It goes further by asking to either delete 27 (3) or to clearly define the competent authority and the binding nature of its decision.[109]

Considering all the uncertainties about this clause, the third-country service providers will refrain from non-personal data transfers, they will try to avoid them and be obliged to store the data in the EU. Having a second data center located in the EU means that they will have extra costs and will have a direct competitive disadvantage in comparison with EU data processing providers and the EU customers will have to pay a higher price. Eventually, this article impedes cross-border non-personal data sharing.[110]

A recent survey by Frontier Economics (commissioned by Computer & Communications Industry Associations (CCIA)) found that 40% of the EU companies think that article 27 of the DA proposal is a *de-facto* ban on data transfers outside the EU from subsidiaries, vendors, affiliates, etc. The remaining 60% of the companies asked to think that it will have

[108] Ibid 71-73.
[109] ACEA, 'Position paper - Proposal for a Data Act' (n 72) 12-13.
[110] Drexl and others (n 93) 74.

implications in their internal operations and increase the cost of compliance by an average of 5% of their yearly global turnover and by 5% for companies whose business model is mainly based on data. Article 27 of the DA proposal is seen as a way to start developing new rules and processes to discriminate against non-EU companies.[111] The restrictions related to non-personal data transfers may lead to a loss of GDP for the EU, but not only. It would also disrupt the way companies operate, collaborate, and innovate.[112]

4.7 FRAND provisions

Fair, reasonable, and non-discriminatory terms (FRAND) is a principle to be applied transparently with regard to data sharing with data recipients. In the context of data sharing, such a principle means that the data shall be made available under the same conditions to comparable categories of data recipients. As mentioned in Chapter 2, data sharing with users will be done free of charge, whereas, for third parties requested by users, it will be done against compensation and under specific rules set in the DA proposal. A dispute settlement body that will be created by each MS, will resolve the disputes based on FRAND. Such a dispute settlement body doesn't have a binding nature, the parties may also decide to go before a judicial.[113] In its adopted position, the Council modifies Article 9 of the proposal and defines specific rules about the interpretation and calculation of FRAND. Furthermore, the Commission shall publish guidelines on how to calculate compensation based on FRAND principles.[114]

FRAND rules are borrowed from the FRAND procedure defined for Standard Essential Patents (SEP). Such a principle is introduced and widely applicable for such cases and developed in relation to competition law. The applicability of these principles in data sharing is still not quite clear. Peter Georg Picht in his paper suggests that the EU should not just copy and paste the competition law rules into the DA proposal. Even though FRAND for SEP has gained some experience, it's still far from perfect, and such shortcomings should not be made part of the DA, considering also the fact that these two

[111] CCIA, 'Data Act: Modest Improvements by EU Parliament and Council Fail To Address Structural Flaws' (*CCIA Net,* 14 March 2023). <https://ccianet.org/news/2023/03/data-act-modest-improvements-by-eu-parliament-and-council-fail-to-address-structural-flaws/> accessed 21 June 2023.

[112] Sarah Snelson, Federico Cilauro, 'The EU has set ambitious targets for the digitalisation of society and business as part of its "Digital Decade" initiative' (*Frontier Economics,* 17 February 2022) <https://www.frontier-economics.com/uk/en/news-and-articles/news/news-article-i9086-eu-data-act-may-carry-significant-costs-for-companies-working-across-borders/> accessed 21 June 2023.

[113] EU Data Act Proposal, arts 8 - 10.

[114] Council of the EU, 'Interinstitutional Negotiations' (n 73) 50 ff, art 9.

have significant differences. Furthermore, he suggests that the DA can be read that FRAND doesn't apply to users, as they receive the data free of charge.[115]

Habich suggests that providing access to data under FRAND terms will incentivize price competition on the side of data holders and they might be willing to share data independently with data recipients. The issue is that different from FRAND terms for SEP, in FRAND for data sharing, the rights of the data holder may not be exclusive, and the data holder does not have ownership of the data, hence not possible to license it. The right to data may also belong to other market participants and the user. The user can limit the access to data, or preclude access to data, hence the data holder can presumably receive a FRAND compensation when possessing a right to retain usage data.[116]

Habich suggests that the obligation for FRAND compensation shall be seen separately from the right of the data recipient to get access to data based on the request of the user. The data should still be shared with the data recipient even in the circumstances when no FRAND compensation has been negotiated, in order to provide more legal certainty. The FRAND compensation terms shall apply only when the parties don't reach a solution (no collaboration during the negotiations).[117]

Another difference between the FRAND for SEP and FRAND for data sharing is that in the case of a patent, it's easier to define what shall be licensed, as the patent is a legal entitlement. In the case of FRAND for data sharing, it is very difficult to map out a data portfolio that shall be shared. Moreover, the data that is required to be shared is not publicly published as it is in the case of patents. The data recipient does not have the option to select what data is generated by the IoT device. Picht states that it's even difficult for the data holder to define what data should be given access to. Another characteristic that makes it even more difficult to define a data portfolio for sharing purposes, is its changing character of data compared to SEP. The portfolio changes much faster in the case of data generated by an IoT device.[118]

---

[115] Picht, 'Caught in the Acts: Framing mandatory data Access transactions under the Data Act, further EU digital regulations acts and competition law' (n 78).

[116] Erik Habich, 'FRAND Access to Data: Perspectives from the FRAND Licensing of Standard Essential Patents for the Data Act Proposal and the Digital Markets Act' (2022) 53 IIC, 1347-1357 <https://ssrn.com/abstract=4119834> accessed 27 June 2023.

[117] Ibid 1360-1361.

[118] Picht, 'Caught in the Acts: Framing mandatory data Access transactions under the Data Act, further EU digital regulations acts and competition law' (n 78) 30.

Picht suggests several approaches in order to enable mandatory data access. He suggests that one approach would be to trust the data holder that it has selected the relevant data to be shared, considering that it's questionable if the data holder can be trusted with the sole remedy, the fear of law. Another approach would be to allow the data recipient to have an overview of the data and select the data that it is eligible to have access based on the DA proposal. The flaws of this approach are that neither competition law, nor the Digital Regulation Acts do not provide the data recipient with such access, and due to the broad exposure of data competition concerns may arise. There is also a proposed solution related to the progress of the technology. Picht suggests that a software solution could be implemented and made part of the IoT device which sorts the data in a way that the relevant data for sharing would be appropriately tagged and transferred to the servers that are designated for mandatory data sharing. Nevertheless, such an option would need further research in order to explore its potential. It can be derived from the above suggestions on handling mandatory data sharing under FRAND terms that adjustment clauses shall be applied in the case of FRAND for data sharing as they are allowed for FRAND for SEP.[119]

[119] Ibid 30-31.

5 Universe of disputes

5.1 Dispute Settlement Body - Article 10 of Data Act proposal

Article 10 of the DA proposal defined the rules for the dispute settlement bodies (DSB) that will cover the disputes in the area of FRAND terms and compensation for data sharing. This clause states that MS will certify bodies that meet certain conditions such as being independent, having the needed expertise to resolve such disputes, being cost-effective, and easily be accessed by data holders and data recipients through electronic communication technology. Such DSBs shall make the fees available before being required by the parties to take a decision. The procedure is assumed to follow certain rules and shall allow the parties to express their opinion regarding the matter, provide statements, and have the option to comment on the statements. The maximum time for taking a decision on the matter is 90 days. The calculator of the deadline starts right after a party has requested a decision on the matter. The decision shall be published and reasoned. The nature of the decision will be binding only if both parties agree to have a binding decision at the beginning of the procedure. In any case, the parties have the right to appear before a court to settle the disputes.[120]

EP in its adopted position, suggests changes to article 10 of the proposal regarding the scope of the disputes, where in addition to the determination of FRAND terms, it will also resolve disputes related to the obligation of the data holder to share data with the data recipient upon the consent of the user. Moreover, the EP adds that the user should also have access to such a dispute settlement body (it was not included in the initial proposal of EC).[121]

In the most recent political agreement between EP and Council, they have agreed to expand the scope of Article 10 even further. They suggest that the customers of the data processing service providers shall also be able to bring disputes before these DSBs, and to settle issues with regards to breach of obligations from such providers.[122]

---

[120] Commission, 'Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)' COM (2022) 68 final (EU Data Act Proposal), art 10.

[121] European Parliament, 'Amendments adopted by the European Parliament on March 2023 on the proposal for a regulation of the European Parliament and of the Council in harmonsed rules on fair access to and use of data (Data Act) (COM(2022)0068 – C9-0051/2022 – 2022/0047(COD))' (Amendments by the European Parliament to the Commission proposal) art 10 <https://www.europarl.europa.eu/doceo/document/TA-9-2023-0069_EN.pdf> accessed 24 July 2024.

[122] European Parliament, 'Provisional agreement resulting from interinstitutional negotiations' (*European Parliament,* 14 July 2023) 76

Tilman and Picht on the other hand, share a similar opinion as EP and Council related to the access of the user in the DSBs as defined in Article 10. Considering the fact that the rights of the third party are derived from the user, they question whether the legislature intended to limit the access of the user to such DSBs. They believe that the user shall have access to the DSB as stated in Article 10 of the DA proposal.[123]

Council has also proposed changes in its adopted position, to article 10. Council suggests that data holders and data recipients shall be able to address and resolve FRAND disputes before DSBs, in accordance with Article 5(8), Chapters III and IV. The Council has expanded the scope of application for FRAND terms. Article 5(8) allows the disclosure of trade secrets with third parties/data recipients, upon the request of the user and only when such a party has put in place measures with a technical and organizational nature to ensure that such trade secrets will be kept confidential. Council states that users shall have the right to file for resolving a dispute before the DSBs only for matters arising out of Articles 4(3a) and 5(8a) which cover the situations in which the data holder refuses to share trade secrets with the user or third party upon the request of the user, after showing that sharing of such trade secrets would cause serious damage to the data holder, despite the measures put in place by user or data recipient. In cases when the outcome of the dispute is positive for the user or data recipient, the data holder would have to reimburse all the fees and reasonable expenses arising out of such a procedure. When the decision is not in favor of the user or data recipient, the user or data recipient does not have any obligations to bear any costs incurred by the data holder, unless the very same DSB rules that the user or the data recipient openly lied or had bad intentions.[124]

Both EP and Council suggest that such dispute settlement bodies publish reports on a regular basis on the number of cases, decisions, the time taken to resolve such disputes, and the most frequent issues they dealt with.[125]

<https://www.europarl.europa.eu/RegData/commissions/itre/inag/2023/07-14/ITRE_AG(2023)751822_EN.pdf> accessed 05 August 2023.

[123] Tilman Niedermaier, Peter Georg Picht, 'FRAND Dispute Resolution under the Data Act and the SEP Regulation' (2023) 4 <https://ssrn.com/abstract=4447930> accessed 14 July 2023.

[124] Council of the EU, '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) - Mandate for negotiations with the European Parliament' (Interinstitutional Negotiations) (2023) 7413/23, 51ff <https://data.consilium.europa.eu/doc/document/ST-7413-2023-INIT/en/pdf> accessed 16 May 2023.

[125] ibid art. 10 (7a).

Despite the changes made to the initial proposal, there are still requests to clarify the nature and the rules for such a dispute settlement body. Irish Business and Employers Confederation (IBEC) states in its position paper that clarity is needed on whether the parties can go to court or tribunal directly or do they have to first try to resolve the dispute through this dispute settlement body as a first step.[126]

Furthermore, many uncertainties have arisen related to the scope and competencies of such DSBs. Article 10 doesn't specify whether such a DSB body covers the cases where the data holder hasn't made an offer to the third party and refuses to share the data. It is also not clear whether it has the competencies and to what extent it can answer any legal questions that might be made by the parties. Tilman and Picht suggest that Article 10 shall be clarified further, especially with regard to the scope and competencies of the DSBs. They recommend that the legislator does not define a narrow scope of disputes, even though this might mean particular expertise and skills for the DSBs. He suggests that Alternative Dispute Resolution (ADR) rules would be a good tool for such alternatives to the judicial solution. Moreover, it seems that the certification requirement of the DSB by the MS is very similar to the one defined in the Consumer ADR Directive in several aspects, even though there are no specific rules in the DA proposal on whether such DSBs can be administrative bodies or standing panels and whether its members will be selected on a case by case from a closed list or if there will be a network of experts. If it will be a closed list, careful considerations shall be taken during the certification process in order not to undermine the independence requirement set in the DA proposal for such DSBs.[127]

The use of ADR for SEP FRAND disputes is also supported by the United States Federal Trade Commission. In their communications, they suggest ADR as a solution for resolving FRAND disputes. Moreover, the courts support this approach as well and consider the arbitration decisions for FRAND. The EU also embraces the ADR as a viable solution for

[126] Irish Department of Enterprise, Trade and Employment, 'Call for views in response to the European Commission's public consultation on the Data Act' (*Enterprise GOV,* 1 April 2022) <https://enterprise.gov.ie/en/consultations/call-for-views-in-response-to-european-commission-public-consultation-on-the-data-act.html>, Ibec Reponse on EU Data Act adoption <https://enterprise.gov.ie/en/consultations/consultations-files/ibec-submission-data-act-consultation.pdf> accessed 24 June 2023.

[127] Niedermaier, Picht, 'FRAND Dispute Resolution under the Data Act and the SEP Regulation' (n 123) 4-7.

resolving SEP FRAND disputes. The practice of the Court of Justice has also demonstrated that the concept of ADR would be acceptable.[128]

As explained above, bringing the dispute before a DSB under Article 10 of the DA proposal does not mean that the decision will be binding, unless both parties have agreed to be binding. It also states that access to such DSB is without prejudice to a party's right to bring the dispute before a court or tribunal. If the matter has been already brought before another DSB or a court, the later DSB shall reject the acceptance/resolution of the dispute (*lis pendens*). It doesn't however mention if such a rule applies if the matter is pending before ADR (e.g., arbitration). Tilman and Picht argue that the same shall apply if a matter is pending in an ADR proceeding. Another question arising about this topic is whether the parties can bring a dispute before a court (in any MS) if such an issue is already pending or being resolved by DSB. Tilman and Picht suggest that if this were allowed, it would diminish the role of the DSB and make it comparable with a 'fragile mediation'. They suggest that in order to preserve the role and importance of the DSB, it should be understood, or the parties shall be able to appeal such a decision before a court or tribunal.[129]

Furthermore, the decisions taken from the DSB shall be recognized by the MS courts, otherwise, no party will address the matter to such DSB if it cannot be enforced. The nature of the DSB bodies is unclear, whether it's a court, an ADR body, or a sui generis body. The legislator shall recognize the decisions at least on the same level as done with arbitration decisions.[130]

5.2 Competent authorities under Data Act proposal

The DA proposal, in Article 31 states that each MS shall define an existing, or a newly established authority to oversee the application and the enforcement of DA. Paragraph 2(a) of this article defines a carve-out regarding the competent authority in relation to chapter VI (switching between data processing services), it specifies that such competent authority shall have expertise in this area. Besides the administrative tasks that this competent authority

[128] Munich IP Dispute Resolution Forum, 'FRAND ADR Case Management Guidelines' (*IDPR Forum,* May 2018) <https://www.ipdr-forum.org/frand-adr-guidelines/> accessed 16 May 2023.
[129] Niedermaier, Picht, 'FRAND Dispute Resolution under the Data Act and the SEP Regulation' (n 123) 10-11.
[130] Josef Drexl and others 'Position Statement of the Max Planck Institute for Innovation and Competition of 25 May 2022 on the Commission's Proposal of 23 February 2022 for a Regulation on Harmonised Rules on Fair Access to and Use of Data (Data Act)' (2022) Max Planck Institute for Innovation and Competition Research Paper 22-05, 43 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4136484> accessed 08 May 2023.

will oversee, it will also be responsible for handling complaints for the violation of the DA, investigating the subject matters, and imposing financial penalties for the violation of the DA. Article 32 specifies that the right to complain is 'without prejudice to any other administrative or judicial remedies'[131] that a party might enjoy.

Council in its adopted position has suggested only a few changes. It suggests adding the requirement that the competent authority in charge of the application and enforcement of chapters 3 and 4 (obligations of data holder to make data available & unfair contractual terms related to data access) shall have expertise in the area of dispute resolution or prices, or ideally both. Moreover, such competent authority will have the obligation to examine the data sharing requests for cross-border data sharing from public bodies, in the circumstances of an exceptional need.[132]

EP, on the other hand, follows a different approach in its adopted text. It comes up with a name for the competent authority by calling it "Data coordinator" and states that such authority shall be the point of contact for the Commission and representing the MS at the European Data Innovation Board. EP specifies further the cooperating and coordinating role of the data coordinator with other relevant bodies and authorities established within the Union. The EP stresses the monitoring role of such authority in comparison with the Commission and Council which define that the competent authority shall be in charge of the application and implementation of the DA. It also includes specific rules about the legal persons that are not established within the Union, the procedure that should be followed by their representatives, or the situations where a legal person is established more than in two EU countries.[133] This procedure seems similar to the one defined in the case of supervisory authorities for personal data.

Important suggested changes have been made by EP in article 32. It limits the right to lodge a complaint only to the situations when there is a suspension of sharing data due to trade secrets.[134] With this clause EP however seems to contradict itself with the provision of article 31 (3b) where there is no limitation on the scope of complaints and investigations it is set to handle. It is unclear whether Article 31 (3b) shall be interpreted as the general rule and 32 as the specific rule.

[131] EU Data Act Proposal, art 31.
[132] Council of the EU, 'Interinstitutional Negotiations' (n 124), arts 31 and 14 (1).
[133] Amendments by the European Parliament to the Commission proposal (n 121), arts 31 and 31 (a).
[134] Ibid art 32.

Moreover, the adopted positions of the EP and Council contradict each other in regard to the disputes handled by Articles 10, 31, and 32. As stated above, in section 5.1, the Council suggests that the disputes arising from Articles 4(3) and 5(8) shall be solved before the DSBs designated for FRAND terms, whereas EP suggests that these disputes are handled by the data coordinator.[135]

Another suggestion that EP brings up and that is neither in the DA proposal nor in the Council's adopted position, is the right of representation via organizations or associations that meet specific criteria, mandated by users, data holders, and data recipients.[136] Furthermore, it also defines the right to appeal the decision taken by the competent authority in charge of overseeing the DA, in cases when the competent authority has taken a binding decision or has failed to provide the parties in a complaint with information on the progress of the case within 3 months from lodging of the complaint. EP goes further and establishes the courts of the MS where the establishment, place or work, or residence of the user is located.[137]

One of the issues of the DA proposal is that it neither accepts nor denies private enforcement as an alternative to an administrative complaint before the supervisory authority (ies) that will be established by MS under Article 31. It is not clear if a user can bring the matter before the civil courts of the MS if a data holder refuses to share the data in accordance with the DA.[138]

Another identified problem that causes confusion is whether a party can lodge a complaint directly with the competent authority over a FRAND terms dispute or should exclusively be filed before the FRAND DSBs that will be established or can a party go directly before an MS court. This question has not been solved by the DA proposal. It's essential to clearly define it in order not to have overlapping tasks between the FRAND DSBs and competent authorities.

5.3 Potential disputes arising out of the Data Act

Personal Data Protection Disputes. The DA proposal states that in all the cases when personal data is concerned, such situations are not subject to the competencies of the

[135] Council of the EU, 'Interinstitutional Negotiations' (n 124), art. 10 and EP adopted position art. 32

[136] Amendments by the European Parliament to the Commission proposal (n 121), art 32a.

[137] Ibid art 32b.

[138] Axel Metzger, Heike Schweitzer, 'Shaping Markets: A Critical Evaluation of the Draft Data Act' (2022) 29-30 <https://ssrn.com/abstract=4222376> accessed 23 June 2023.

competent authority in charge of the application and implementation of DA, instead will be handled by the designated supervisory authority under the GDPR.[139]

As mentioned in this paper already, one of the issues with the DA Proposal is how to know from the start if personal data is involved or not and how to deal with the mixed data sets (personal and non-personal data that cannot be split). Should there be two open proceedings in such cases, one before a competent authority under the GDPR, for personal data and one case for non-personal data (the competent authority under Article 31)? It is not clear how such disputes will be resolved and whether these disputes can be resolved separately.

Trade secrets disputes. As it is not that clear from the TSD, quite often it is not possible to determine what data constitutes trade secrets. Kerber argues that data holders can consider many things as trade secrets and require far-reaching confidentiality obligations in place. It is very challenging to determine from the start whether certain data fall within the trade secrets umbrella, and there is no way to find that before litigation.[140] There will also be disputes from refusal to disclose trade secrets at all if the data recipient doesn't have in place the technical and organizational measures to protect trade secrets, and who assesses such measures.

Disputes about the amount and use of data. As described in section 4.5 of this paper, it is not easy to assess what data should be generated or collected from an IoT device and what amount of data can be shared with the user and the recipient of the data. Disputes might arise in this topic, especially if manufacturers of IoT devices will try to limit access to data for specific reasons. About the same topic, there might arise disputes on the purpose of using the data. As the data can be shared with the data recipient (third party), when requested by user to be used only as per consent given by the user, if such a data recipient utilizes the data beyond the scope agreed with the user, this will be addressed for dispute resolution. The data holder may as well dispute based on the intent behind the data request - the reason for asking for data.

Public institutions disputes. As permitted under the DA proposal, under exceptional circumstances the data shall be shared with public bodies and union institutions. The disputes that might arise here could be twofold, from the data holder arguing that the conditions are not met to make the data available, and from the public authorities if the data

[139] EU Data Act Proposal, art 31 (2a).

[140] Wolfgang Kerber, 'Governance of IoT Data: Why the EU Data Act will not fulfill its objectives' (2023) 72 (2) GRUR International, <https://doi.org/10.1093/grurint/ikac107> accessed 29 April 2023.

holder refuses to share a certain amount of data. Considering that the nature of the DSB under Article 10 and Article 31 of the DA proposal is not specified, there could be a risk that if these institutions that will be designed or certified by MS will be other public bodies, the criteria of impartiality may not be met when it comes to disputes that concern share of the data with public bodies or government.

Disputes from smart contracts. DA proposal allows the data holder to apply a smart contract under certain conditions to prevent unauthorized access to data. When the data holder deploys such contracts for the purposes of data sharing, among other criteria that it should fulfill is that it should be designed in a way to enable parties to pause its execution, be it through suspension or termination of such contract.[141] Industry specialists believe that this rule shakes the foundation of smart contracts by requesting the pause button and goes against the nature of such contracts.[142] It is not clear how disputes arising out of the suspension or termination of such contracts will be solved. If they fall under the scope of Article 31 of the DA proposal, it's not specified whether such committee/competent authority will have the necessary expertise and experience to provide resolution.

Disputes from unfair contractual conditions. Chapter IV of the DA proposal enables SMEs to disagree with unfair contractual terms when the bargaining power between the negotiating parties is disproportionate. The scope of disputes that might arise under this chapter would be related to the determination of unfair contractual terms, and who can decide on this matter.[143]

Other disputes. Another case that is not clear is how and where would a dispute be resolved where a party has more than one claim (e.g., one about FRAND compensation and the other one refers to the violation of the DA). It could be that the parties file two complaints (one with DSB for FRAND terms and another one with the competent authority). It seems that there are no complications in this case if the disputes can be filed in two different designated bodies, but in practice, it could be that the disputes cannot be separated because the outcome of one issue may impact the other issue. Cross-border disputes would also be a challenging topic considering that there is worldwide data flow.

---

[141] EU Data Act Proposal, arts 11 and 30.

[142] Ledger Insights, 'EU Data Act requires smart contracts to have kill switch, not be permissionless' (*Ledger Insights,* 14 March 2023) <https://www.ledgerinsights.com/eu-data-act-smart-contracts-immutability-permissionless/> accessed 4 July 2023.

[143] EU Data Act Proposal, art 13.

6 Information and protocols to help with dispute resolution

6.1 Flaws on the Data Act related to dispute resolution

As described in section 5.1 of this paper, there are already a lot of uncertainties with regard to the DSBs that are to be designed by member states to handle FRAND disputes. It is unclear whether FRAND for data disputes will be as problematic as FRAND for SEP was at the beginning when it was introduced. The fact that these bodies will be certified by each MS might result in rules that are not uniform across MS but instead very different in every MS, which might affect the effectiveness of the tool. It is also not clear if the parties bring the claim directly before an MS court, whether the decision of the FRAND DSBs will be recognized by the courts, or if the court will not consider it at all. Furthermore, given the short deadline that is given for resolving the dispute, it is not specified what are the consequences if the dispute is not resolved within the given deadline. The nature of the DSB is not clearly defined and there is the risk that some MS define its nature as an ADR body, some others as a sui generis body.

The second institution in charge of overseeing infringements arising out of the DA (except for FRAND terms) is the one defined in Article 31 of the DA proposal. The nature of such bodies and the power of their decisions are also not clear. As mentioned in section 5.2 of this paper, it's unclear if the parties can bring the issue directly before a court of an MS or if they should first have it reviewed by the competent authority. It seems that there might as well be some overlapping or confusion between the tasks defined for resolving FRAND disputes and the rest of the disputes. Furthermore, the intention of the EU legislators to create two different bodies and have them in charge of different matters it's not fully clear. The rationale for this could have been the expertise on FRAND disputes. If this was the purpose of the EU, then the question that arises is whether FRAND could have been incorporated as a commission or division within the competent authority that will be designed under Article 30. Would this not mean fewer resources needed to have a functioning system?

Another question arising regarding the disputes is whether the designated authorities will be able to cope with the nature of the disputes, given the fact that it's a new law that is being implemented for the first time in the EU. Will these authorities have the necessary resources to ensure effective implementation, safeguarding, and dispute settlement? What could the legislator change in order to effectively use the resources and at the same time

ensure that the DA is being effective and minimizing the number of disputes? The most important points to be considered in this situation will be described in section 6.2 below.

6.2 Framework for a dispute settlement system

A big question when we see the scope of disputes under the DA, is how member states will be able to resolve all the disputes that may arise from the DA. As this act will largely affect individuals, businesses, and governmental & public bodies, the system shall be designed in a way that is not overwhelmed by requests or complaints, especially given the deadlines for resolving the disputes given to the DSBs under the DA.

When designing a dispute settlement system, it is important to assess and define the following elements: goals that the system wants to reach, stakeholders and their importance, in what culture and context will such a system function and how does culture contribute to efficiency, which are the processes and structure to be applied for resolving of the disputes, resources made available to make it work, and if the system is successful or not, it is monitored and properly assessed on the progress.[144]

The goal of the dispute settlement system:[145] It can be extracted that the main goal of the system would be to handle the disputes in a cost and time-effective manner and through certain methods (e.g., electronic communication tools)[146] to enable and empower users (non-business users) to get access and be in control of the data generated by their use of IoT devices. The system shall also be able to handle a large number of disputes. Moreover, it's important to have the necessary experience on the matter, so the system does not create legal uncertainties and is able to establish trust in the DA. The main types of disputes will consist of business-to-business and business-to-consumer disputes. It is however not clearly defined whether the goal of the system is to bring a good number of disputes to litigation, to have them resolved in administrative ways/bodies, or through ADR. It is vital to make clear what

[144] Lisa Amsler, Janet Martinez and Stephanie Smith, *Dispute System Design: Preventing, Managing, and Resolving Conflict* (Stanford University Press 2020) ch 2 <www.sup.org/books/cite/?id=17595> accessed 3 July 2023.

[145] The structure below (goal, stakeholders, context and culture, process and structure, resources, success, accountability, and learning) is taken from the framework provided in the book *'Dispute System Design: Preventing, Managing, and Resolving Conflict'* authored as specified in reference n 140.

[146] Commission, 'Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)', COM (2022) 68 final (EU Data Act Proposal), art 10.

are the goals of the system to be able to define whether one standard process (arbitration, mediation) shall apply, or many options shall be given.[147]

Moreover, it can be argued that an array of process options could be beneficial due to the various nature of disputes that might arise, but also due to the international character of disputes. As the task and functions of the competent authorities described in Article 31 seem quite extensive, it appears very unlikely that such authorities established within each MS to have expertise in each and every area of a dispute that might arise (especially with a law that it's first of its kind in the EU and the nature and amount of the disputes, cannot be accurately estimated). Having the option to choose between ADR or the competent authorities, the one that might have more comprehensive expertise for certain disputes would make the parties feel more comfortable with the outcome of the process. At times, it can also contribute to making the situations less complicated. For instance, in the case of a dispute where mixed data sets are involved, it would be much easier (process, time, and cost-wise) for all parties in a dispute to approach a specialized ADR body rather than having a complicated process where parts of the dispute will be handled by the competent authorities (non-personal data) and parts of it by personal data protection supervisory authorities (personal data).

The expertise of the DSBs is crucial in the case of trade secrets disputes as well. The legal and business expertise are essential to the parties in order to receive a fair, fast, and professional judgment. As already discussed in this paper, the TSD itself is not that clear on what is considered a trade secret, and quite often businesses tend to classify lots of information as trade secrets in order to provide them with high protection. Legal expertise and good knowledge of the TSD would be essential in the case of such disputes. Unless the competent authorities would include special committees for various types of disputes e.g., for trade secrets disputes (which could be a costly approach and probably applied differently in different MS), it would make sense that parties refer the case to an ADR body that is specialized in handling these disputes.

Technical expertise is also of a particular importance that would require specialized dispute bodies for resolving the disputes. Having the option to choose the DSB that has more experience and good knowledge on the disputes related to the amount of data that could/should be shared with the user or the data recipient, and the particular sector/industry

[147] Amsler, Martinez, Smith (n 144) ch 2.

would be beneficial for parties and could lead to a higher level of satisfaction and certainty for all parties.

Other elements that might be of significance with regards to process options are trust, costs and time efficiency. For some parties/stakeholders the main priority could be having a time efficient process outcome, for other stakeholders of a particular size could be more important low costs, the rest might consider more important trust on the body that resolves the dispute. Hence, the presence of process options would help each stakeholder to align with their priorities.

Methods for resolving disputes are important especially for international dispute resolution. Article 10 of the DA proposal suggests that all FRAND disputes shall be resolved by using electronic communication tools. Nevertheless, the same obligation is not included in the case of the process that is to be followed by competent authorities under article 31 of the DA proposal. It would be an added value in the case of cross-border disputes to have the option to resolve them via the electronic communication tools. It would be less costly for both parties (eliminate traveling costs, and other associated costs), the dispute can be resolved faster, and depending on the process, maybe the parties don't even have to confront each other if they don't want to. Use of electronic communication tools in a dispute would potentially increase access to justice as well as it's easier for the parties to raise a dispute in comparison with filing it before a certain authority and having to be present before certain authorities.

The goal of the currently established process allows the parties to go before the court and ask for preliminary judgements when there is a question regarding the interpretation of the law. However, this process works only when a dispute is brought before the national court of the MS. The MS court may then refer the case to the European Court of Justice (ECJ), where an interpretation of law in relation to the question is provided.[148] As it is expected that many questions and interpretations may be needed due to the new and special nature of this legislation, the Commission may want to consider an alternative option to include an advisory opinion process for the cases that don't get resolved before a MS court. Such an advisory opinion process could probably be given by a committee within the competent authorities, with legal expertise, especially in the field of data. Such a solution would

[148] EUR-Lex, Preliminary ruling proceedings - recommendations to national courts', (*Eur-lex,* 26 April 2022) <https://eur-lex.europa.eu/EN/legal-content/summary/preliminary-ruling-proceedings-recommendations-to-national-courts.html> accessed 02 August 2023.

probably provide in a time efficient manner interpretation of the DA, from experts in this very particular field and contribute to reducing the workload of the ECJ.

However, an array of process options would increase the risk of inconsistency (inconsistent interpretations and decisions) across different DSBs, and MS. Considering the nature of the EU (multicultural and different systems in every MS), this risk is always present. In this case, the risk could be mitigated with the reporting obligations of the DSBs (the number, nature and outcome of disputes). The legislator could use the information from reporting to come up with guidelines to reduce inconsistency. Moreover, the right to appeal the decision taken by a DSB, in a MS court, would also reduce the inconsistencies because such decisions can always be brought for interpretation before the ECJ.

Stakeholders: As discussed in Chapter 3 of this paper, there are many stakeholders involved such as businesses (in the quality of a data holder, manufacturer, or user), consumers as users of IoT devices), governments, and union institutions, universities, NGOs, etc. Having so many stakeholders also mean different positions, power, and interests. As analyzed in this paper, even though the DA proposal seems user-centric and intends to empower the users, it appears often that de facto the manufacturer or the data holder has more bargaining power and the ability to meet one-sided decisions. It is questionable why the data holder/manufacturer would want to give consent to the binding nature of the decision based on FRAND terms (as per article 10 of the DA proposal) if they are the party that has to perform obligations. There seems to be no incentive for the data holder/manufacturer. What could be the worst that could happen if the data holder does not provide the user or the third party with the data? Would a user/third party (natural persons) go to an MS court every time that the data holder/manufacturer or will it remain unpunished most of the time? It is difficult to provide answers to these questions, but it would certainly be helpful to include incentives in the process for the party that has more bargaining power or make available remedies that can easily be enforced by users (cost and time effective).

Context and culture: Both the DSBs for FRAND and the competent authority (ies) that will be designated for resolving or handling the disputes/complaints, will be different in every MS. Each MS has the freedom to certify the bodies under Articles 10 and 31, which, taken into consideration cultural differences, might lead to different rules for the system in every MS and different handling of disputes. The element of language also plays a role. As there are many languages spoken within the EU, it also implies that a translator will be involved in the process in the case of cross-border disputes, especially if the parties will have

the opportunity to provide statements and reply to statements.[149] By giving the MS the freedom to define the nature of the DSBs under Article 10 and designate competent authorities as per Article 31, it would lead to non-uniformities of the system within the EU, which could potentially affect the effectiveness of the system. It would be suggested that the EU Commission draws some guidelines on the nature of the DSBs/competent authorities in order to facilitate the process for the MS and take into consideration cultural differences and approaches to the topic of the data.

Processes and structure: Process plays an important role in dispute resolution. Generally in a dispute settlement system one or more processes, which may be linked or not together, have different purposes, (e.g. fast resolving of the disputes, cost-effective, etc.) and intend to include or empower specific stakeholders in the process.[150] It can be suggested that the purpose of the process for FRAND disputes is to have a process with an independent dispute body, that is cost-effective and is able to resolve the disputes via electronic communication methods within 90 days.[151] On the other hand, the purpose of the process for the competent authority under article 31 of the DA proposal seems to be safeguarding the DA (overseeing infringements, enforcement), complaint handling, and investigating and sanctioning those who violate it.[152]

It is important to define the processes in a way that is not confusing and provides legal certainty. As there are two different processes for handling disputes/complaints, there should not be overlapping of tasks. The current process under the DA does not provide clarity on whether in the case of a FRAND dispute, the parties shall refer the dispute to a DSB (under article 10 of the DA proposal) or they can submit a complaint with the competent authority as specified in articles 31 & 32 of DA proposal at the same time or can directly head for litigation in an MS court. Even though Amsler, Martinez, and Smith in their book highlight the importance of giving the parties the right to choose a process when there is more than one process, as it provides the user with the feeling that the process is fair,[153] it's necessary in this case to have these choices aligned together in order not to create any confusion and controversies. This can be done by recognizing the decision taken and defining the nature of the decisions for each dispute/complaint body in a clearer way and also explicitly stating

[149] EU Data Act Proposal, art 10.
[150] Amsler, Martinez, Smith (n 144) ch 2.
[151] EU Data Act Proposal, art 10 (2).
[152] Ibid, arts 31 and 32.
[153] Amsler, Martinez, Smith (n 144) ch 2.

that if a matter is filed before a DSB body/competent authority/court if a later one receives it, it should reject it.

Resources: When designing a DSD, resources that are available for the implementation are a key point. If there are not enough resources available, the process may not be able to achieve its goals.[154] It is not clear what are the needed resources to achieve the goals set in the DA proposal. For complaints filed before the competent authority that will be designated by each MS, it is not mentioned any costs to be paid by the party that lodges a complaint. However, it is stated that the MS have the obligation to equip the authorities in charge with the necessary resources to perform the obligations set in the proposal.[155] If the resources will not be detailed and estimated accordingly prior to the formation of such competent authorities, it again may lead to non-uniformities in the handling of the complaints across MS as such MS may make available different resources (budget, personnel, tools), which might affect the speed of the process, efficiency, etc. Furthermore, the DA proposal gives the MS the freedom to either create one or more new competent authorities or task authorities that are already established.[156] Defining such authorities may depend on the importance that each MS wants to give to such legislation, it could be that the choice of the MS will be heavily influenced by the resources to be made available.

For the FRAND disputes, there are several cost types included. As the MS will have to certify the DSBs in accordance with the DA requirements,[157] MS will need a certain body to support the certification (could be an existing one or establish a new certification body). In any case, this will result in costs for the MS. DSBs on the other hand, will also incur costs in relation to the certification as they would have to at least adapt their organization in accordance with the requirements of the DA proposal. And then there are costs for the process when a dispute is brought before a DSB. DSBs are required to make such costs public and transparent before the parties request a decision. [158] However, the DA proposal itself does not specify which party should pay the costs of the process. Council in its adopted position has suggested that the costs shall be covered by the data holder when the decision is against the data holder and in addition, it will have to pay the user, or the data recipient other reasonable expenses incurred during the process. When the decision is in favor of the

[154] Amsler, Martinez, Smith (n 144) ch 2.
[155] EU Data Act Proposal, art 31 (7).
[156] Ibid art 31 (1).
[157] Ibid art 10 (2).
[158] Ibid art 10 (4).

data holder, the user or the data recipient does not have to compensate back the expenses or the fees to the data holder, each party covers its expenses, except for the cases when the user or the data recipient act in bad faith. [159] This process seems to treat the user and data recipient and Council seems to recognize the de facto power of the data holder.

Success, Accountability, and Learning: Amsler, Martinez, and Smith argue that a measure of success is not just achieving the goals set for such a system, but broader goals related to the society such as justice and fairness. It is important to evaluate a system in many ways and check if it is properly working, the stakeholders are happy about it, it is transparent, and credible, and invites the participants to give feedback.[160] As the DA is still in the proposal phase and has not become law yet at the time of writing this paper, it's difficult to evaluate if the system is working. In the initial DA proposal from the Commission, there are not included any elements to help measure success. However, in its adopted position, the Council has included reporting obligations of the FRAND DSBs with regards to the number of disputes, time taken to resolve them, the outcome and what were the most common disputes brought before such bodies.[161]

Regarding the competent authorities under the DA proposal, there are not included any public reporting obligations for such authorities. It's not clear how and whether these authorities will measure the elements of success, accountability, and learning. Furthermore, the system is not designed in a way to ask for users' direct feedback. It is not known whether the legislator will develop such a measurement element at a later stage or intends to not measure it at all.

6.3 Potential scenarios for dispute resolution

Examining the flaws of the DA proposal in regard to dispute handling and analyzing them as per a given DSD framework is an important piece in order to come up with different suggestions that might potentially improve these flaws. There are several scenarios that might address the concerns and flaws mentioned in this paper.

[159] Council of the EU, '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) - Mandate for negotiations with the European Parliament' (Interinstitutional Negotiations) (2023) 7413/23, 51ff <https://data.consilium.europa.eu/doc/document/ST-7413-2023-INIT/en/pdf> accessed 16 May 2023.
[160] Amsler, Martinez, Smith (n 144) ch 2.
[161] Council of the EU, 'Interinstitutional Negotiations' (n 159) 52, art 10 (7a).

Scenario 1: Provide clarity and transparency for the current dispute settlement systems

This solution would probably be the easiest one as not many changes would be needed in the proposed dispute systems. The legislator could provide more information on handling the disputes arising out of Articles 10 and 31 of the DA proposal. It would also be essential that the Commission publishes guidelines to help the MS establish the bodies stated in these articles, in order to ensure uniform application of the DA. Uniform application and implementation will increase the chances of an effective dispute resolution system.

Furthermore, in order to manage the amount of disputes, and not overwhelm MS courts or competent authorities, it is important to define that the nature of the DSBs established for FRAND terms, is binding and will be recognized by MS courts in order to increase its credibility of DSBs and not turn it into 'fragile mediation'.[162] The suggestion of the Council in its adopted text for defining who is responsible for covering the costs arising out of a dispute would also be helpful and make the system more user-friendly and take into consideration lower-income parties.

As mentioned in this paper, the rules for handling FRAND disputes resemble the rules defined in the Consumer ADR directive.[163] The Commission could include wording in the proposal that if there are ambiguities in Article 10 with regards to procedure or rules, the procedure and the rules defined in the Consumer ADR directive shall be taken into consideration where applicable.

With regards to the competent authority (ies), the legislator shall clarify if it's mandatory to bring the dispute first before the competent authority or if the parties can go directly before the MS court. The suggestion of the EP that the MS courts serve as an instance for appeal of the competent authority decision,[164] shall be incorporated in the DA proposal.

Scenario 2. Expand the scope of disputes to be handled by DSBs under article 10

Another scenario would be to expand the scope of disputes that can be handled by the DSBs

[162] Tilman Niedermaier, Peter Georg Picht, 'FRAND Dispute Resolution under the Data Act and the SEP Regulation' (2023) 10-11 <https://ssrn.com/abstract=4447930> accessed 14 July 2023.

[163] Ibid 4-7.

[164] European Parliament, 'Amendments adopted by the European Parliament on March 2023 on the proposal for a regulation of the European Parliament and of the Council in harmonsed rules on fair access to and use of data (Data Act) (COM(2022)0068 – C9-0051/2022 – 2022/0047(COD))' (Amendments by the European Parliament to the Commission proposal) <https://www.europarl.europa.eu/doceo/document/TA-9-2023-0069_EN.pdf> accessed 24 July 2024.

under article 10[165]. This would mean reducing the risk of overloading the system with complaints and dispute-resolving requests which can be expected to be in considerable amounts given the fact that it's the first law of this nature to be introduced in the EU and wider. There are many unknowns for the parties and taking into consideration the stakeholder positions analyzed in chapter 3, there are also different interests. Different stakeholders highlight many uncertainties about this proposal. Expanding the scope of disputes to be handled by the DSBs (ADR bodies) there would be needed an increase in the transparency. These DSBs would have to report on the cases they resolve, the outcome, nature of the cases, industries and most common issues faced.

Giving the DSBs power to resolve a wider range of disputes, would also mean fewer requests before the competent authority (probably no need for establishing new authorities but distributing those tasks to existing authorities), and therefore fewer resources are needed for handling the disputes and complaints. As MS will be certifying these DSBs, there could be interest from existing ADR DSBs to get certified and hence cover a large number of disputes within an efficient time frame. Competent authorities under Article 31 would need experts or specialized teams to deal with each type of dispute (e.g., smart contract disputes).

Empowering of DSBs with a wider scope of disputes would also speed up the process and provide decisions faster, especially with the use of technology as specified in Article 10, by using electronic communication tools. The disputes could be resolved with the help of Online Dispute Resolution (ODR), where the system could be designed in a way that certain disputes (low contract value) are resolved with the help of technology (automated) and without a person physically having to deal with the dispute (e.g., disputes about smart contracts[166] or disputes about compensation amount for making data available to a data recipient). Furthermore, the use of ODR would be vital for resolving cross-border disputes, which might be the case very often. ODR can as well offer experts in different areas, depending on the nature of the disputes.

As Amsler, Martinez, and Smith argue in their book, by giving the user/parties the opportunity to choose between different dispute resolution options (e.g., litigation, arbitration, mediation, etc.) the chances that the system is more effective are higher. The

[165] EP also has suggested expanding the scope of disputes - see chapter 5.

[166] Kleros offers a solution where the presence of the parties is not needed. More information is here <https://kleros.io/>

user tends to believe that when they have the choice there is transparency and the decision is fairer.[167]

Another upside for using ADR in such disputes would be in the cases of mixed data sets. Prof. de Werra in his paper suggests that the wording included in the GDPR implies the use of ADR for resolving disputes arising from personal data portability. The use of ADR, in this case, would help the designated supervisory authorities to cope with the workload and move away from the traditional judgments and instead shift it online. An online dispute resolution would be more convenient in terms of costs but also in terms of the length of the proceedings. Prof. de Werra suggests that the development of such a uniform ODR mechanism would help in resolving disputes about personal and non-personal data. Furthermore, he states that in today's environment, the mixed data sets will be present quite often, hence the coordination between different regulatory regimes is important.[168] There is no suggestion that personal data disputes are non-arbitrable. Moreover, this has not been denied, instead, the EU accepted the arbitration mechanism related to the privacy shield.[169] The ADR that was initially applied for transnational personal data disputes has shown effectiveness and that it works, despite the fact that the privacy shield is not active anymore between the EU and the U.S.[170]

The downside of expanding the scope of disputes for the DSB under article 10, would be the risk of different interpretations and positions on the DA. There would be interpretations from DSBs that potentially will have a nature very similar to ADR, with different positions from competent authorities, and from MS courts.

Moreover, if many disputes will be solved via ADR, it could be an option a multi-stakeholder monitoring body (could be incorporated within the competent authorities), where representatives from main stakeholders would be part of. Such body could analyze on annual or semiannual basis the scope of disputes brought before ADR, the practical flaws of the legislation, challenges, the outcome of the cases and suggest how to improve moving forward. It would be reasonable that such body works on rotation (limited mandates) and

[167] Amsler, Martinez, Smith (n 144) ch 2.

[168] Jacques de Werra, 'Using Arbitration and ADR for Disputes about personal and non-personal data: What lessons from recent developments in Europe?' (2019) 30 (1) ARIA 201-202 <https://www.digitallawcenter.ch/sites/default/files/publications/unige_134313_attachment01.pdf> accessed 14 July 2023.

[169] Ibid 203.

[170] Ibid 206.

have adaption skills over time based on certain dynamics. The presence of a multi-stakeholder monitoring body would help in identifying right away the main challenges arising in practice and solving them with the knowledge of industry experts and keeping them satisfied.

Scenario 3. Transferring FRAND DSBs competences to competent authority (ies)

In order to make the dispute settlement process less complicated and reduce the number of resources for the implementation and enforcement of the DA proposal it would be an option to transfer the competences of the FRAND DSBs to the competent authority (ies) designated under Article 31 of the DA proposal. It requires certain expertise to handle such complaints, but so does the switching of cloud providers, or handling requests related to the share of data with public institutions. It could be a separate division of committee with the necessary expertise for determination of FRAND terms. MS would not have to certify these institutions and make the process less confusing for all the parties involved. The competent authority (ies) designated would then be similar to a central authority for handling all issues related to DA. Alongside lodging the complaint before the competent authority would also be the option to go to ADR for resolving disputes. The parties would have the option to choose whether they want to file a complaint with the competent authorities or arbitration, mediation, etc. The litigation in the MS courts is recommended to be used for appealing the decision of the competent authority (ies) or a decision coming out of ADR.

7 Results and Conclusion

7.1 Results

The DA proposal came as a result of EU strategy for data in the course of technological developments in the EU and worldwide and the increasing role of data for the benefit of the economy. The EU has conducted market studies and researched the potential of unlocking the data and ensuring that such data freely flows within the EU. Another driver for coming up with this law is the dependency of EU businesses in data processing service providers, which at the moment is being dominated mainly by non-EU companies (approximately 75 % market share from U.S. companies).

The scope of the DA proposal is to enable mandatory data sharing between businesses, business to consumer, business to public institutions of MS (in exceptional circumstances). The data holder (which is not always the manufacturer) will be obliged to share the data derived from an IoT device or related services with the user (which can be a business or natural person/consumer) and with the third parties when requested by the user. The shared data can be used only for specific purposes that will be agreed between the user and data recipient. Sharing of data with the user will be free of charge whereas with the data recipient towards a fair, reasonable and nondiscriminatory compensation in the case of third parties. Furthermore, the DA proposal will facilitate switching between different data processing service providers. Cloud providers will be obligated to offer certain support for their customers (based on reasonable charges) in order to facilitate switching of providers within a reasonable timeframe.

Data that will be made available to users and third parties will be the data produced by the IoT device or related services. As the data will be shared for free (no compensation involved) with the user, the data holder has only the responsibility to provide the data in a raw format (without investing time and putting efforts to make the data available) but able to be accessed by the user, in an up-to-date form, accurately. The user seems to be in control of the data created or collected by the IoT device and related services. The manufacturers are tasked with designing the product in a manner that enables the user to access its data. This has become object to discussion as many authors recognize the de facto control of the manufacturer and even though the user seems to be in the center of the DA proposal, the manufacturer is the party that is in control of data, designs the product and gets to decide what data shall be shared with the user. It is understood that the data will be shared through

an agreement involving the user, the third party and the data holder. Such a contract has however of an unclear nature and is not specifically described in the DA proposal. The DA seems to affect more sectors/industries such as data processing sector, automobile industry, manufacturing.

Many different stakeholders with different interests and positions have published position papers regarding DA. Different groups of stakeholders have different concerns on the DA proposal. There is legal uncertainty among businesses concerning share of data, such as the data ending up in the hands of competitors, if the data will be safeguarded and type and the amount of data to be shared, modalities for data sharing, etc. On the other hand, public institutions seem to be satisfied and find data sharing in case of public emergencies very helpful. Consumers on the other hand demand more control on the data generated by them.

Based on the position papers and interpretations of several academics, there are identified several potential problems about the DA proposal. One of the biggest issues is the requirement for the data holder to provide trade secrets to the user, third parties and public institutions when requested by the user or public institutions. Data holders seem concerned as this may lead to unfair competition, expose their business information out there, their trade secrets, which potentially might harm competition and future innovation. In contrast, there are authors that argue that by not including it as an obligation, it might lead to rejection of data sharing hiding under the TSD. Furthermore, it's not even clear what is trade secret under the directive. To strike a balance, during the trilogue, Council and EP has suggested adding additional safeguards when it comes to sharing of trade secrets, to ensure that the necessary confidentiality agreements, technical and organizational measures are in place prior to sharing of such trade secrets.

Another major issue seems also to be the case of mixed data sets (personal and non-personal data sets). The personal data protection authorities seem concerned about such situations claiming that it might lead to personal data breaches. It is not always possible to know from the start if personal data is involved. They believe that there will be confusion and coordination between the supervisory authorities under GDPR and competent authorities for DA will be needed. International data transfers are also identified as a problematic sphere. The restrictions set in Article 27 for many stakeholders are a barrier in international data transfers. Setting a similar regime for international non-personal data transfers like for the personal data is seen as not a proportional tool to achieve the goal.

Article 10 of the DA proposal has also been subject to discussions between academics. Borrowing FRAND terms concept from FRAND for SEP and applying it in the case of data sharing is seen as not entirely appropriate. It appears that FRAND for SEP has not resulted without problems during the implementation phase. The EU Commission, EP, and Council also have different positions regarding the scope of the disputes that this body shall be responsible for. The nature of the DSBs is not specified, even though it is very similar to the ADR, the DA proposal doesn't say if it will be ADR. The nature of the decisions is also not entirely clear. Article 10 suggests that decisions shall be mandatory only if the parties agree in advance to be mandatory. It's questionable what would be the purpose of settling a dispute before the DSBs if the outcome is not mandatory to the parties. It is unclear whether the parties shall first bring the dispute before DSBs, or if they can go directly before the MS courts. Furthermore, the certification from different MS might lead to non-uniform application within the EU.

The DA proposal states that each MS shall designate one or more authorities (existing or newly established) to overlook the enforcement, application, and infringements.[171] The nature of such 'competent authorities' is not clear. They will handle complaints, investigate, provide decisions within a reasonable timeframe, and set financial penalties when the parties infringe the law. In this case, it is also unclear whether the parties can go directly to the court or first file the disputes with these authorities. Some of the disputes foreseen to arise out of the DA are disputes related to personal data and mixed data sets, trade secret disputes, disputes about the amount and use of data, disputes for sharing data with public institutions, disputes from smart contracts, etc.

Furthermore, the author has applied the framework for a dispute settlement system suggested by Amsler, Martinez, and Smith in their book, to analyze and identify the flaws with the current dispute settlement system in the DA proposal. Elements of the framework such as the goal of the system, stakeholders, context and culture, resources, success, accountability, and learning have been analyzed. The goals of the system are not clear, there seem not to be any priorities in the goals. There are also flaws in the process and structure. There is no information on how much resources shall be made available to establish such dispute settlement systems.

[171] Commission, 'Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)', COM (2022) 68 final (EU Data Act Proposal), art 31.

7.2 Conclusions

The main findings of this research are as follows:

There is a big interest in this piece of legislation. Stakeholders seem concerned about personal data involved in data sharing, sharing of the data with public institutions, protection of IP rights (including trade secrets), what amount of data and what the specific data will be shared with the user or data recipient, switching between cloud providers and international non-personal data transfers. The provisions on these topics are unclear.

The process for resolving disputes is also not clear. There are designated two dispute resolution bodies (DSBs for FRAND terms and competent authorities in each MS). Nevertheless, the nature of their decisions is not clearly defined. It's not clear if the parties can go before a MS court directly or should they first file the complaint before these bodies. Furthermore, there is the risk of non-uniform rules and application across MS, if there are not more specific guidelines on this topic. The topic of data sharing may be considered of different importance for different MS; hence they might allocate different amounts of resources.

To answer the research question on what kind of protocols, and information flows will help prevent, diagnose, and resolve the disputes arising from the EU DA:

- Legislators shall provide more clarity on the scope of the DA, what data shall be generated from an IoT device and then be shared with the user (or data recipient).
- Trade secrets is one of the topics that most businesses are concerned about and there is a lot of legal uncertainty around it. The legislator shall limit the share of trade secrets only under certain circumstances, when necessary to achieve the goals, provided that the goal cannot be achieved otherwise. In practical terms, the information will be shared with many users. It would be hard to find out, or prove which user disclosed the trade secrets, if it was shared with a large number of users. At the same time, such limitations shall not strengthen the position of data holders and be a cause for abuse of position from data holders. It is about finding the right balance.
- When enabling mandatory data sharing (breach of which comes with financial sanctions for businesses), there should also be taken into consideration practical aspects of such data sharing and balance the potential gains and losses coming from such a decision, especially when it might affect international trade. Putting in place similar legal regimes for both personal and non-personal data might create barriers,

and potentially be burdensome for business. Taking into consideration that today's business environment has become more international, differentiating the regimes that apply to these two categories of data would be helpful in day-to-day business operations.

- EU Commission shall come up with guidelines prior to the implementation of the regulation in order to help MS design a process that is uniform across MS so it can build the foundation of an effective system
- For resolving the disputes and having an effective system, there are three possible scenarios. First scenario would be to provide clarity and transparency to the currently designed dispute system, especially regarding the binding nature of the decisions. In order for such a dispute system to work, it would be necessary that the decisions are recognized and enforceable. Second scenario would be to expand the scope of disputes that DSBs designated for FRAND disputes under article 10. Expanding the scope of disputes, would give the parties more choices for dispute settlement and at the same time would manage the number of disputes and not overwhelm the system. The idea of a multi-stakeholder monitoring body would help to set a balance during the implementation of this proposal. The third scenario would be to transfer the competences of DSBs for FRAND to competent authorities that will be designed under Article 31. Such a solution would help in reducing resources. Alternatively, the parties should be able to have the option to go for ADR.

This research is limited to topics related to the research question. It doesn't examine in depth the user rights under the DA, nor the technical and organizational measures to be implemented by users, or data recipients when trade secrets are shared. Even though it is briefly touched upon on the mechanisms for sharing data, it would be recommended further research about the contracts for data sharing and how such contracts would work in practice (where at least three parties are involved). This will be beneficial to stakeholders during the implementation phase. Research on the type and amount of data that can/should be shared with the user and the data recipient under the DA, in different sectors or industries would also be valuable guidance. The representatives of different sectors have already a lot of uncertainties about their role and obligations concerning the DA.

8 Bibliography

-Academic sources

Amsler L, Martinez J, Smith S, D*ispute System Design: Preventing, Managing, and Resolving Conflict* (Stanford University Press 2020) ch 2 <www.sup.org/books/cite/?id=17595> accessed 3 July 2023.

Casolari F, and others, 'How to Improve Smart Contracts in the European Union Data Act' (2023) 2 (9) *DISO* <https://doi.org/10.1007/s44206-023-00038-2> accessed 14 May 2023.

Colangelo G, 'European Proposal for Data Act - A First Assessment' (2022) Centre on Regulation in Europe Evaluation Paper, 20-21 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4199565> accessed 04 June 2023.

De Werra J, 'Using Arbitration and ADR for Disputes about personal and non-personal data: What lessons from recent developments in Europe?' (2019) 30 (1) ARIA 201-202 <https://www.digitallawcenter.ch/sites/default/files/publications/unige_134313_attachment01.pdf> accessed 14 July 2023.

Drexl J, and others 'Position Statement of the Max Planck Institute for Innovation and Competition of 25 May 2022 on the Commission's Proposal of 23 February 2022 for a Regulation on Harmonised Rules on Fair Access to and Use of Data (Data Act)' (2022) Max Planck Institute for Innovation and Competition Research Paper 22-05, 3-5 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4136484> accessed 08 May 2023.

European Law Institute, 'ELI submits a response to the EU Commission's Public Consultations on the Data Act' (*European Law Institute,* 03 September 2023) 21-23 <https://europeanlawinstitute.eu/news-events/news-contd/news/eli-submits-a-response-to-the-european-commissions-public-consultation-on-the-data-act/> accessed 16 June 2023

Habich E, 'FRAND Access to Data: Perspectives from the FRAND Licensing of Standard Essential Patents for the Data Act Proposal and the Digital Markets Act' (2022) 53 IIC, <https://ssrn.com/abstract=4119834> accessed 27 June 2023.

Kerber W, 'Governance of IoT Data: Why the EU Data Act will not fulfill its objectives' (2023) 72 (2) GRUR International <https://doi.org/10.1093/grurint/ikac107> accessed 29 April 2023.

Kop M, 'The Right to Process Data for Machine Learning Purposes in the EU' (*Standord Law School,* November 2020) <https://law.stanford.edu/wp-

content/uploads/2020/11/Mauritz-Kop_The-Right-to-Process-Data-for-Machine-Learning-Purposes-in-the-EU.pdf> accessed 14 June 2023.

Metzger A, Heike Schweitzer, 'Shaping Markets: A Critical Evaluation of the Draft Data Act' (2022) 29-30 <https://ssrn.com/abstract=4222376> accessed 23 June 2023

Niedermaier T, Picht P, 'FRAND Dispute Resolution under the Data Act and the SEP Regulation' (2023) 4 <https://ssrn.com/abstract=4447930> accessed 14 July 2023.

Picht P, 'Caught in the Acts: Framing mandatory data Access transactions under the Data Act, further EU digital regulations acts and competition law' (2022) Max Planck Institute for Innovation& Competition Research Paper 22-12 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4076842> accessed 13 June 2023.

Rotenberg M, 'ELI Webinar on the Data Act: How to Boost the European Data Economy?' (*European Law Institute,* 24 May 2022) (Webinar) <https://europeanlawinstitute.eu/news-events/upcoming-events/events-sync/news/eli-webinar-on-the-data-act-how-to-boost-the-european-data-economy-2/?tx_news_pi1%5Bcontroller%5D=News&tx_news_pi1%5Baction%5D=detail&cHash=3f711f21c32dc495d4cc864440b66a75> accessed 16 May 2023.

-EU law and documents

Commission, 'Accompanying Commission Staff Working Document - Impact Assessment Report', SWD (2022) 34 final <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022SC0034&from=EN> accessed 4 February 2023.

Commission, 'Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)' COM (2022) 68 final (EU Data Act Proposal).

Commission, 'Public Consultation on the Data Act: Summary Report' (*EU Commission,* 06 December 2021) <https://digital-strategy.ec.europa.eu/en/library/public-consultation-data-act-summary-report> accessed 07 May 2023.

Commission, European Innovation Council and SMEs Executive Agency, 'Study on the legal protection of trade secrets in the context of the data economy – Final report' (Publications Office of the European Union, 2020) 2-3 <https://data.europa.eu/doi/10.2826/021443> accessed 3 June 2023.

Council of the EU, '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) - Mandate for negotiations with the European Parliament' (Interinstitutional Negotiations) (2023) 7413/23 <https://data.consilium.europa.eu/doc/document/ST-7413-2023-INIT/en/pdf> accessed 16 May 2023.

Council Regulation (EU) 2022/1925 of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 [2022] OJ L265/28.

EDPB, EDPS, 'Joint Opinion 02/2022 on the Proposal of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)' (*EDPS,* 4 May 2022) 2 <https://edps.europa.eu/system/files/2022-05/22-05-05_edps-edpb-jo-data-act_en.pdf> accessed 13 March 2023.

European Parliament, 'Amendments adopted by the European Parliament on March 2023 on the proposal for a regulation of the European Parliament and of the Council in harmonsed rules on fair access to and use of data (Data Act) (COM(2022)0068 – C9-0051/2022 – 2022/0047(COD))' (Amendments by the European Parliament to the Commission proposal) <https://www.europarl.europa.eu/doceo/document/TA-9-2023-0069_EN.pdf> accessed 24 July 2024.

European Parliament, 'Provisional agreement resulting from interinstitutional negotiations' (*European Parliament,* 14 July 2023) <https://www.europarl.europa.eu/RegData/commissions/itre/inag/2023/07-14/ITRE_AG(2023)751822_EN.pdf> accessed 05 August 2023.

-Websites

ACEA, 'Position paper - Proposal for a Data Act' (*ACEA,* 16 May 2022). <www.acea.auto/publication/position-paper-proposal-for-a-data-act/> accessed 9 May 2023.

Bertuzzi L, 'Industry associations ask EU policymakers to pull the breaks on Data Act' (*Euractiv,* 03 February 2023) <www.euractiv.com/section/digital/news/industry-associations-ask-eu-policymakers-to-pull-the-breaks-on-data-act/> accessed 08 May 2023.

BEUC, ‘Data Act important for competition and consumer choice’ (*BEUC,* 23 February 2022) <https://www.beuc.eu/press-releases/data-act-important-competition-and-consumer-choice> accessed 9 May 2023.

CCIA, ‘Data Act: Modest Improvements by EU Parliament and Council Fail To Address Structural Flaws’ (*CCIA Net,* 14 March 2023) <https://ccianet.org/news/2023/03/data-act-modest-improvements-by-eu-parliament-and-council-fail-to-address-structural-flaws/> accessed 21 June 2023.

Commission, ‘Data Act - Questions and Answers’ (Questions and Answers) (2022) <https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_1114> accessed 4 February 2023

Commission, ‘Data Act: Commission proposes measures for a fair and innovative data economy’ (Press Release) (2022) <https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113> accessed 4 February 2023.

Commission, ‘Shaping Europe’s digital future: Commission presents strategies for data and Artificial Intelligence’ (Press Release) (2022) <https://ec.europa.eu/commission/presscorner/detail/en/ip_20_273> accessed 18 March 2023.

De Cordier T, and others, European Parliament and Council ready to start trilogue negotiations on EU Data Act - European Data law is getting closer’ (*CMS Legal,* 29 March 2023) <https://news.cms.law/rv/ff00a7d1d0e3e1cf20dbf2caae4f85e46bbe647e> accessed 6 May 2023.

Digital Europe, ‘Data Act agreement: The necessary balance is yet to be achieved’ (*DIGITALEUROPE,* 28 June 2023) <https://www.digitaleurope.org/news/data-act-agreement-the-necessary-balance-is-yet-to-be-achieved> accessed 29 July 2023.

Digital Europe, ‘Rebalancing the Data Act’ (*DIGITALEUROPE*, 01 September 2022) <https://www.digitaleurope.org/resources/rebalancing-the-data-act/> accessed 25 May 2023.

DOT Europe, ‘DOT Europe publishes position paper on Data Act’ (*DOT Europe,* 04 May 2022) <https://doteurope.eu/news/dot-europe-publishes-position-paper-on-data-act/> accessed 21 May 2023.

EUR-Lex, 'Preliminary ruling proceedings - recommendations to national courts', (*Eur-lex,* 26 April 2022) <https://eur-lex.europa.eu/EN/legal-content/summary/preliminary-ruling-proceedings-recommendations-to-national-courts.html> accessed 02 August 2023.

European Parliament, 'Data Act, Legislative Train Schedule' (*European Parliament,* 23 June 2023) <www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-data-act?sid=7101> accessed 21 July 2023.

Guerzoni F, 'Digital Transformation: Underestimating the Data Act's impact on trade secrets' protection will undermine European industrial competitiveness' (*Oraglim,* 17 January 2023) <https://orgalim.eu/position-papers/digital-transformation-underestimating-data-acts-impact-trade-secrets-protection> accessed 14 March 2023.

Guerzoni F, Digital Transformation: Joint Statement - The Data Act is a leap into the unknown' (*Oraglim,* 1 February 2023), <https://orgalim.eu/position-papers/digital-transformation-joint-statement-data-act-leap-unknown> accessed 14 March 2023.

Insurance Europe, 'Response to EC consultation on Data Act proposal' (*Insurance Europe,* 17 May 2022) <https://www.insuranceeurope.eu/publications/2606/response-to-ec-consultation-on-data-act-proposal/> accessed 10 May 2023.

Irish Department of Enterprise, Trade and Employment, 'Call for views in response to the European Commission's public consultation on the Data Act' (*Enterprise GOV,* 1 April 2022) <https://enterprise.gov.ie/en/consultations/call-for-views-in-response-to-european-commission-public-consultation-on-the-data-act.html>, Ibec Reponse on EU Data Act adoption <https://enterprise.gov.ie/en/consultations/consultations-files/ibec-submission-data-act-consultation.pdf> accessed 24 June 2023.

Irish Department of Enterprise, Trade and Employment, 'Call for views in response to the European Commission's public consultation on the Data Act' (*Enterprise GOV,* 1 April 2022) <https://enterprise.gov.ie/en/consultations/call-for-views-in-response-to-european-commission-public-consultation-on-the-data-act.html>, Vodafone Position Paper on EU Data Act <https://enterprise.gov.ie/en/consultations/consultations-files/vodafone-submission-data-act-consultation.pdf> accessed 10 May 2023.

Ledger Insights, 'EU Data Act requires smart contracts to have kill switch, not be permissionless' (*Ledger Insights,* 14 March 2023) <https://www.ledgerinsights.com/eu-data-act-smart-contracts-immutability-permissionless/> accessed 4 July 2023.

Munich IP Dispute Resolution Forum, 'FRAND ADR Case Management Guidelines' (*IDPR Forum,* May 2018) <https://www.ipdr-forum.org/frand-adr-guidelines/> accessed 16 May 2023.

Naujokaitytė G, 'EU Data Act is causing friction' (*Science Business,* 11 May 2023) <https://sciencebusiness.net/news/eu-data-act-causing-friction> accessed 21 June 2023

Naujokaitytė G, 'EU is poised to give industry a data boost – and universities want in' (*Science Business,* 14 March 2023). <https://sciencebusiness.net/news/Data/eu-poised-give-industry-data-boost-and-universities-want> accessed 14 May 2023.

Snelson S, Cilauro F, 'The EU has set ambitious targets for the digitalisation of society and business as part of its "Digital Decade" initiative' (*Frontier Economics,* 17 February 2022) <https://www.frontier-economics.com/uk/en/news-and-articles/news/news-article-i9086-eu-data-act-may-carry-significant-costs-for-companies-working-across-borders/> accessed 21 June 2023.

Synergy Research Group, 'European Cloud Providers Continue to Grow but Still Lose Market Share' (*Synergy Research Group,* 27 September 2022) <https://www.srgresearch.com/articles/european-cloud-providers-continue-to-grow-but-still-lose-market-share> accessed 4 February 2023.

Wirth A, Tricco G, Martinez M, 'Clouds on the Horizon: Europe's Cloud Policy threatens transatlantic digital harmony' (*CEPA,* 10 May 2022) <https://cepa.org/article/clouds-on-the-horizon-europes-cloud-policy-threatens-transatlantic-digital-harmony/> accessed 14 June 2023.