
# CiTiP Working Paper Series

## White Paper on the Data Act Proposal

**Edited by**

**Charlotte Ducuing**
**Thomas Margoni**
**Luca Schirru**

CiTiP Working Paper 2022

KU Leuven Centre for IT & IP Law - imec

26 October 2022

# White Paper on the Data Act

## Table of Contents

## Abstract

The Data Act proposal of February 2022 constitutes a central element of a broader and extremely ambitious initiative by the European Commission to regulate the data economy. CiTiP's Data Act White Paper, which is based and expands on a coordinated series of blog posts published by CiTiP during the summer of 2022 (https://www.law.kuleuven.be/citip/blog/category/data-act-series), attempts a first detailed analysis of the various provisions of the Data Act in light of this broader policy and regulatory landscape. This is done by putting on centre stage one of the main objectives of the EU Data Strategy: the creation of a single market for data or, in other words, the creation of European Data Spaces.

This White Paper discusses the Data Act Proposal as published by the European Commission on 23 February 2022. At the time of writing, this proposal is under discussion both at the European Parliament (currently by the Working Party on Telecommunications and Information Society) as well as at the EU Council under the Czech presidency which is working on a new compromise text. Given that at the time of closing this analysis (25 October 2022) no new official texts have been published, the following analysis refers to the EC proposal of February 2022.

## Keywords

Data regulation; Data access; Data portability; Data sharing; Data Spaces; Data-driven technologies; FRAND; Internet of Things; Interoperability; Machine-generated data; Data Act; Data Strategy; data intermediary; data governance.

## Acknowledgments and contributors

The Centre for IT & IP Law (CiTiP) at the Faculty of Law and Criminology, University of Leuven (KUL) is a consortium member of the Data Space Support Centre (https://dssc.eu), a Digital Europe Program project funded by the European Commission (Grant Agreement number: 101083412) with the goal of exploring the needs of data space initiatives, define common requirements and establish best practices for European Data Spaces. Prof. Thomas Margoni is PI for KUL.

Contributors to the White Paper

**Aliki Benmayor:** Researcher at Centre for IT & IP Law (CiTiP), KU Leuven, Belgium; H2020 MobiDataLab project, funded by the EU under the H2020 Research and Innovation Programme (grant agreement No 101006879).

**Antoine Petel:** Doctoral researcher at the Université Jean Moulin, France.

**Athena Christofi:** Doctoral Researcher at Centre for IT & IP Law (CiTiP), KU Leuven, Belgium; SPECTRE, an interdisciplinary project funded by Research Foundation – Flanders. This project has received funding from FWO, Research Foundation – Flanders – FWO reference number S006318N.

**Bert Peeters:** Researcher at Centre for IT & IP Law (CiTiP), KU Leuven, Belgium; imec Smart City initiative City of Things.

**Charlotte Ducuing:** Doctoral researcher at Centre for IT & IP Law (CiTiP), KU Leuven, Belgium; C2 interdisciplinary KU Leuven research project 'Datafication of the Circular Economy'.

**Daniela Spajić:** Doctoral researcher at Centre for IT & IP Law (CiTiP), KU Leuven, Belgium; H2020 LaST-JD-RIoE project, funded by the EU's H2020 Research and Innovation Programme under Marie Skłodowska-Curie Actions (grant agreement No 814177).

**Elisabetta Biasin:** Doctoral researcher at Centre for IT & IP Law (CiTiP), KU Leuven, Belgium; In Silico World project, funded by the EU under the H2020 Research and Innovation Programme (grant agreement No 101016503).

**Ella De Noyette:** Doctoral researcher at Centre for methodology of law and Centre for IT & IP Law (CiTiP), KU Leuven Kulak, Belgium. Her research is currently funded by KU Leuven Kulak. As of the first of November, her PhD research will be supported by the Research Foundation – Flanders (FWO).

**Emre Bayamlıoğlu:** Researcher at Centre for IT & IP Law (CiTiP), KU Leuven, Belgium.

**Eyup Kun:** imec- Doctoral Researcher at Centre for IT & IP Law (CiTiP), KU Leuven, Belgium; H2020 ENSURESEC project, funded by the EU under the H2020 Research and Innovation Programme (grant agreement No 883242.).

**Jingyi Chu:** Visiting researcher at Centre for IT & IP Law (CiTiP), KU Leuven, Belgium; PhD candidate at China University of Political Science and Law.

**Julie Baloup:** European Commission, Belgium.

**Leander Samuel Stähler:** Doctoral researcher at Centre for IT & IP Law (CiTiP), KU Leuven, Belgium.

**Luca Schirru:** Postdoctoral researcher at Centre for IT & IP Law (CiTiP), KU Leuven, Belgium; Skills4EOSC project. Skills4EOSC has received funding from the European Union's Horizon Europe research and innovation Programme under Grant Agreement No. 101058527.

**Maria Avramidou :** Researcher at Centre for IT & IP Law (CiTiP), KU Leuven, Belgium; H2020 PRAETORIAN project, funded by the EU under the H2020 Research and Innovation Programme (grant agreement No 101021274).

**Teodora Lalova-Spinks:** Doctoral researcher at Centre for IT & IP Law (CiTiP), KU Leuven, Belgium. Teodora's PhD research is supported with a scholarship awarded by the Research Foundation–Flanders (FWO), Project No. 11H3720N. Clinical Pharmacology and Pharmacotherapy, Department of Pharmaceutical and Pharmacological Sciences, KU Leuven, Belgium.

**Thomas Gils:** Researcher at Centre for IT & IP Law (CiTiP), KU Leuven, Belgium; legal & policy researcher at Knowledge Centre Data & Society.

**Thomas Margoni:** Research Professor of Intellectual Property Law at the Faculty of Law and Criminology, KU Leuven, and a member of the Board of Directors at the Centre for IT & IP Law (CiTiP).

# Executive Summary

The Data Act proposal of February 2022 constitutes a central element of a broader and extremely ambitious initiative by the European Commission (EC) to regulate the data economy. CiTiP's Data Act White Paper, which is based and expands on a series of blog posts published on CiTiP's blog during the summer of 2022 (https://www.law.kuleuven.be/citip/blog/category/data-act-series), attempts a first detailed analysis of the various provisions of the Data Act in light of this broader policy and regulatory landscape. This is done by putting on centre stage one of the main objectives of the EU Data Strategy: the creation of a single market for data or, in other words, the creation of European Data Spaces. In this Executive Summary, we offer an overview of the Data Act proposal (1), a summary of the analysis performed in the White Paper (2), then we highlight the key policy recommendations that emerged from the analysis (3) and, finally, we conclude by highlighting some of the core regulatory and policy findings (4).

## Overview of the Data Act proposal: Policy objectives

The Data Act Proposal consists of ten substantive chapters (and one dedicated to final provisions). Each chapter aims to fulfil specific objectives, as stated by the EC in its Explanatory Memorandum. This section offers a brief overview of the core objectives and corresponding chapters.

a. *"Facilitate access to and use of data by consumers and businesses, while preserving incentives to invest in ways of generating value through data"*

This objective is operationalised in Chapters II to IV (chapter I elucidates subject matter, scope and definitions). Chapter II lays down rules concerning access and use of IoT products' data (B2B and B2C data sharing). The stated goal is to empower IoT product users vis-à-vis IoT product manufacturers (also known as 'data holders') with respect to such data. Chapter III is constructed as a general regulatory framework applicable to data holders legally obliged to make data available. A clear – yet implicit – connection with future European Data Spaces, for which more specific data sharing obligations may be adopted (such as in the case of the European Health Data Space Regulation) is palpable. Finally, Chapter IV aims to articulate the principle of fairness in B2B commercial data transactions, although this is only to the benefit of small and medium-sized enterprises (SMEs).

b. *"Provide for the use by public sector bodies and Union institutions, agencies or bodies of data held by enterprises in certain situations where there is an exceptional data need"*

Such objective relates to Chapter V, which aims to allow public sector bodies to require access to data held by the private sector (B2G data sharing) to address situations of so called 'exceptional needs', which plausibly cover emergencies such as the Covid pandemic.

c. *"Facilitate switching between cloud and edge services" ('data processing services')*

Chapter VI aims to addresses some enduring lock-in vendor issues in cloud computing, which were left unsolved by the 2018 Free-Flow of Non-Personal Data Regulation.[1] With carefully selected words, the latter Regulation laid down an 'encouragement' for cloud computing service providers to develop self-regulatory codes of conduct expected, in turn, to 'facilitate' the switching of service providers and the porting of data from one to the other.[2] With the Data Act proposal, the EC engages much more decidedly with a detailed set of rules which effectively amount to a 'right to switching'.

d. *"Put in place safeguards against unlawful data transfer without notification by cloud service providers"*

This objective forms part of the broader digital sovereignty strategy of the European Union.[3] The 'safeguards' and more generally the regulation of international data transfer by data processing service providers, are regulated as per Chapter VII.

e. *"Provide for the development of interoperability standards for data to be reused between sectors"*

In this respect, Chapter VIII lays down an ambitious framework for further European Commission regulatory interventions concerning data (services) interoperability. Interoperability speaks directly to the needs and operations of European Data Spaces.

f. *"Enforcement"*

Chapter IX requires Member States to establish yet again 'competent authorities' to ensure the application and enforcement of the Data Act substantive provisions, with the additional objective to ensure consistency between the various data-related legal frameworks.

g. "*Clarifications relating the Sui Generis Database Right and IoT generated data*"

Finally, the short Chapter X intends to clarify the scope of the SGDR in relation to IoT generated data as defined and regulated in Chapter II.

## Summary of analysis

The **introduction** of the White Paper contextualised the theoretical framework within which the analysis has been developed. This included the broader policy structure of the EU Data Strategy and the role of the Data Act and other instruments of EU Data Law. The introduction finally identified four general recurring themes in the Data Act and, more generally, in the public discourse regarding the EU data strategy: (1) Fixing well-known issues in data markets: A pragmatic approach; (2) Unleashing the value of privately held data: Data Spaces; (3) Innovative approaches: data in the public interest, data sharing and data co-generation; and (4) Regulatory interfaces: The Data Act and other areas of information law.

**Sec. 2** of the White Paper focused on IoT data access and sharing obligations as regulated in Ch 2 of the Data Act. It focused on so-called defensive and positive facets of 'data control' that the Data Act is expected to guarantee for the user of an IoT product or related service.

**Sec. 3** of the White Paper analysed the topic of data portability contained in the Data Act in relation to other legal instruments, such as the GDPR, the DGA and the proposal for a European Health Data Space Regulation, with a focus on the empowerment of individual rights.

**Secs. 4 and 5** of the White Paper examined Chapter III of the Data Act, assessing, on the one hand, the appropriateness of the FRAND terms as conditions for future obligations to make data available (Article 8) and the interpretative uncertainties of the provisions on technical protections measures (Article 11), on the other hand.

**Sec. 6** of the White Paper builds a conceptual bridge between Chapters III and IV of the Data Act and offers an overview of the B2B sharing and access rules in the cases of contractual (Chapter III) and statutory (Chapter IV) obligations to make data available and the role of the fairness test of Article 13.

**Secs. 7-9** of the White Paper discussed Chapter V of the Data Act. First, Sec. 7 dealt with the general concept of B2G data sharing. It analysed the "what, who, when and how" of these obligations and raised a (first) number of questions on the scope of B2G sharing. Then, Sec. 8 dived into the 'exceptional need' concept. Finally, Sec. 9 provided a case study, setting out the need for data-sharing for smart city development and the possibilities the Data Act creates.

**Sec. 10** of the White Paper focused on a specific aspect of Chapter VI, that is, the obligations of data processing service providers to remove obstacles to and assist their users in effective switching between providers, or in other words, to the 'right to switch'.

**Secs. 11-12** of the White Paper discussed Chapter VII and the international access and transfers of data. Article 27 provides safeguards against unlawful access and transfers to non-EU countries, prohibiting certain transfers and obliging the providers to take 'all reasonable measures' to prevent those transfers. While the first contribution of this section gave a general overview of the Article, the second contribution discussed similarities and differences with the existing regulatory landscape, in particular, the GDPR and the DGA.

**Sec. 13** of the White Paper covered Chapter IX of Data Act on enforcement measures. The Data Act requires Member States to establish two new types of enforcement authorities: the 'dispute settlement bodies' and the respective 'competent authorities' and grants supplementary competences to the 'European Data Innovation Board', already set up by the DGA.

**Sec. 14** of the White Paper discussed Chapter X of the Data Act, which offers a much-needed clarification on the relationship between IoT data and the sui generis database right (SGDR), in particular by 'clarifying' that the SGDR does not apply to IoT data.

**Sec. 15** of the Data Act addressed the complex relationship between the Trade Secrets Directive and the Data Act. Both instruments try to facilitate information sharing, but the TSD does this by protecting the shared information rather than obliging the sharing itself.

**Sec. 16** of the White Paper develops a case study on the relationship between the Data Act and medical devices. The Section considered the definitions of 'data holder', 'user', and 'data' in a complex medical device data sharing scenario and identified interpretational difficulties. As health data is also a concern of other legislative initiatives, such as the GDPR, the EHDS, the (In-Vitro) Medical Device Regulation, the NIS Directive and the Cybersecurity Act, part 16 also discussed the interplay with these initiatives.

The **Conclusions** of the White Paper identified several areas of policy and regulatory attention both within the Data Act proposal and across the broader field of data regulation or EU Data Law. These areas, given their importance, are presented below in Sec. 3 of this Executive Summary.

## Summary of policy recommendations

The White Paper developed a detailed article-by-article (or Section) analysis of the Data Act proposal. In the below table we summarise the main recommendations that the authors of each section have formulated with the intention of offering an external and independent scientific input to the law-making process. They are grouped into four main categories: Terminological clarification, Synergy with other laws, Internal harmonisation/classification, addition/removal of obligation.

| Type of recommendation | Chapter of the Data Act Proposal | Recommendation |
|---|---|---|
| **Clarification** | Chapter I | In the definition of 'Data holders': Clarify the exact meaning of 'through control of the technical design of the product and related services'. |
| **Clarification** | Chapters I and V | Consider removing public authorities from the definition of "data holder" (of the Chapter 5) to clarify the "B2G" and "G2G" frameworks. |
| **Clarification, improvement** | Chapter II | Clarify and ensure the downstream effect of Article 4(6), second sentence and clarify that the data portability right under Article 5 is not subject to exhaustion. |
| **Internal harmonisation** | Chapter II | Regulate further the alignment between the data 'offer' by the data holder and the data 'demand' by the third party chosen by the user under Article 5, by laying down, for instance, specific transparency requirements to the benefit of chosen third parties. |
| **Clarification** | Chapter III | FRAND terms should be clarified in many aspects, including the subject matter of FRAND terms and the compensation (in particular, whether data are covered or not) and what is meant by 'making data available'. |
| **Removal of an existing obligation, improvement** | Chapter III | Article 8(6) should be object of a careful re-drafting as it is currently not well coordinated both taxonomically and systematically with the other provisions and the Data Act and of the TSD. |
| **Improvement, simplification** | Chapter V | Given the close relationship between response, prevention and recovery of public emergency, the differences in the respective legal regimes might be unnecessary (that is, the requirement of "limited in time and scope" in article 15(b) and compensation in article 20). |
| **Clarification** | Chapter V | In relation to "major cybersecurity incidents (public emergencies)": Clarify the meaning of 'major' cybersecurity incidents and consider more broadly the potentials of including cybersecurity within the scope of the Data Act. |
| **Synergy with other laws, concepts and bodies** | Chapter VI | Regulate the interface between Chapter VI and the Digital Content Directive, for example, based on sui generis rules concerning the conformity requirements for switching. |
| **Clarification** | Chapter VII | Clarify the legal nature of the opinion of the competent body or authority on whether the conditions for non-personal data access/transfer are fulfilled and in particular whether such opinion is binding or not. |

| | | |
|---|---|---|
| **Synergy with other laws, concepts and bodies** | Chapter IX | Insofar as competent authorities shall be established by member States, regulate further the conditions in which they shall cooperate between the respective enforcement authorities. |
| **Removal of an existing obligation** | Chapter IX | Remove the obligation of competent authorities and DPAs to 'seek consistency' when enforcing the Data Act. |
| **New obligation** | Chapter X | In order to give it full and clear legal effect, the obligation contained in Recital 63 should be moved and/or restated in the main body of the Act (i.e., as an Article). |
| **Clarification** | Chapter X | Remove the first part of Article 35 and place it in Rec. 84 to help eliminating any possible doubt relating to the scope of the exclusion. |
| **Synergy with other laws, concepts and bodies** | Chapter X | Clarify that "For the purpose of Article 7 Database Directive, IoT data as defined in the Data Act are created data and, therefore, as such have never been object of SGDR protection". |
| **Clarification** | Data Act | Consider exploring (informal) procedural guarantees to protect the user against artificial blocks of sharing requests by the data holder in relation to ex ante v. ex post determination of Trade Secret. |
| **Synergy with other laws, concepts and bodies** | Data Act | The terminology employed to enshrine the new versions of the right to data portability under the Data Act and EHDS proposals shall be unified, and the legal and technical interoperability between the various applicable laws shall be guaranteed. |

## Summary of findings

In this part, we offer a reasoned summary of the main wide-ranging findings of the White Paper.

A broader data strategy. The Data Act proposal is only one, albeit key, piece of the wider EU Data Strategy. Other core elements of this initiative are the Data Governance Act (DGA), the Public Sector Information (PSI)/Open Data Directive (ODD), and the Regulation on the Free Flow of Non-Personal Data (FFNPDR). Additional initiatives designed to regulate digital services (the Digital Services Act or DSA), digital markets (Digital Markets Act or DMA), artificial intelligence (AI Act), the extraction of informational value from protected works (CSDM) and the processing of personal data (GDPR) may be seen as part of a renewed interest in a coordinated approach to the regulation of digital and data-intensive technologies. A complete understanding of this novel area of law – EU Data Law – cannot be achieved without assessing all these policy and regulatory interventions in their entirety.

EU values at the core. The EC demonstrates profound awareness and ambition of global leadership in setting up what could be termed as the new gold standard in the relationship between data and digital technologies. The EU frames this relationship around a set of core values that include a competitive and functioning single market (not unexpectedly the legal basis of all these interventions) as well as fairness, proportionality, accountability, and transparency. This represents an important, yet not entirely, feature of the legislation here discussed. It explicitly embodies in the regulation of data and connected technology some of the Charter's fundamental rights, for example, personal data and the privacy of communications, intellectual property rights, consumer protection, the right to use and

dispose of lawfully acquired possessions, the rights of children as vulnerable consumers, freedom to conduct a business, freedom of contract, as well as fair and effective protection against unfair contractual terms. The resulting framework may be represented as a model of governance between pure market and a fully regulated approach combining elements that traditionally belong to private law and public law domains. Within this broader context, digital sovereignty acquires crucial significance as an enabler of the goals to be achieved.

A pragmatic approach. Within the above-sketched framework, the Data Act proposal purports to enable and promote the creation of value from data, especially privately held data, clarifying entitlements, conditions, and procedures along three main types of interactions: Business to Consumers (B2C), Business to Business (B2B) and Business to Government (B2G). This is done following two main legislative methods. First, the EC purports to fix several data-related issues, such as data-driven foreclosures of markets and abuse of dominance in the field of IoT products as well as cloud and edge computing, therefore focusing essentially on B2B interactions. Second, the Data Act proposal intends to advance a political project for the European data economy to create more value and innovation from data exchange and re-use, here focusing on all three interactions. This second approach reveals one of the most ambitious undertakings of the EC Data Strategy: the realisation of European Data Spaces.

No to data property. To achieve the intended strategic results (competition, value creation, fair data exchanges and innovation), and despite some initial demands in the opposite sense, the chosen way has not been that of a recognition or extension of additional (intellectual-) property rights in data, or, in other words, that of a property-based approach. This is another defining element of the EU data strategy.

Yes to data governance. The question of how to reach and release the value contained in privately held databases remains. In fact, whereas the Open Data Directive (ODD) enacts a detailed set of rules on the reusability of High Value Datasets, of research data and of other data held by Public Sector Bodies (PSBs); and while the DGA extends those approaches – in the form of recommendations – to data held by PSBs that are excluded from the ODD, a similar approach, albeit theoretically conceivable, would have been difficult to implement for privately owned datasets. This would have necessarily taken the form of some sort of positive obligation to make available privately held databases, with the potential to encroach upon property and competition principles.

European Data Spaces. The road chosen by the EU is innovative, inspired, far-reaching and takes the name of European Data Spaces. In other words, the creation of a mixed public-private regulatory space will offer the infrastructural and regulatory framework within which data, including privately held datasets, will be voluntarily exchanged, or made available following an obligation to do so, for economic and societal benefit. This will effectively become what has been termed the European single market for data. By doing so, the EC aims to foster data sharing and re-use, which is expected to deliver growth and innovation, support policy making and preserve European values such as privacy, property, competition, consumer protection, pluralism, safety, security, fairness, ethical standards and digital sovereignty.

Data Portability. 'Data portability' is gaining traction as the means to fix market failures and empower the respective beneficiaries. However, as it is well known, data portability will only deliver on expectations – if at all – provided that interoperability is guaranteed. This essential lesson learned from the application of the data portability right under the GDPR, shifts the focus from portability to

the regulation of interoperability as a key factor. Accordingly, it may be necessary to warn against over-expectations from "simple" data portability provisions. This calls for further decisive initiatives, possibly as part of additional regulatory interventions in the field of European Data Spaces.

Agile regulation. With the double objective to enable the law to keep pace with innovation and to allow experimentation, regulatory sandboxes have become a major theme in the field of law and technology. It is, therefore, no surprise that regulatory sandboxing is expressly referred to in the European Data Strategy.5 More recently, the AI Act has aimed to foster the use of regulatory sandboxes, viewed as a novel form of agile regulatory oversight and a safe space for experimentation, in order to support innovation. However, 'agile regulation' also brings significant challenges to the foundations of Law, which should be monitored and assessed in the light of the reported EU core values.

Independent authorities. The Data Act may be seen as constituting an instance of the broader trend of the EU lawmaker to the recourse to dedicated independent administrative enforcement authorities. As Sec. 13 of the White Paper shows, this regulatory trend is not without considerable consequences. The centrality attributed to independent authorities in the EU Data Strategy demands a reflection on the need for a renewed theory of the role and legitimacy of such authorities in the EU and of the kind of administrative and judicial oversight that they should be subjected to.

Data intermediaries. Criticism has already been raised in the literature about the unclear relationship between the DGA and the Data Act.6 This is particularly the case concerning the role that data intermediaries, governed by the Chapter III of the DGA, could play to facilitate Chapter II of the Data Act. It is not easy to position data intermediaries in relation to the various stakeholders, for instance as the 'chosen third party' (the beneficiary of the data portability right) or as playing yet another role, or both. We formulate the hypothesis that data intermediaries could play a role as facilitators of the legal regime laid down in Chapter II. One of the key goals of the Data Act is to allocate data fairly within the stakeholder value chain. Especially under Chapter II, this implies to navigate the rights and legitimate interests of several actors, and in particular within the triangular relationship formed by the data holder, the user and the chosen third party. Data intermediation could certainly be a much needed enabling service.

International context. Data flows travel to and from countries across and outside the EU. It seems arguable that the challenges that the Data Act and the broader EU Data Strategy aim to address are global and thus not confined within the EU borders. However, the EU approach to data governance is strongly grounded on the idea of embedding EU values in it. It will certainly be interesting to monitor the future global developments in this area and to observe whether, like in the case of the GDPR for data protection, the Data Act could also become a role model for data governance across the globe.

# 1 Introduction – Charlotte Ducuing[1] and Thomas Margoni[2]

## 1.1 The Data Act within the digital legislative package

The Data Act proposal of February 2022 constitutes a central element of a broader and extremely ambitious initiative of the European Commission (EC) to regulate the data economy. Other core elements of this initiative are the DGA,[3] the Public Sector Information (PSI)/Open Data Directive,[4] and the Regulation on the Free Flow of Non-Personal Data (FFNPDR),[5] even though the latter predate one of the key policy documents in the field, the European Data Strategy of 2020.[6] Additional initiatives designed to regulate digital services (the Digital Services Act or DSA),[7] digital markets (Digital Markets Act or DMA),[8] Artificial Intelligence (AI Act),[9] the extraction of informational value from copyright works (CSDM)[10] and the processing of personal data (GDPR)[11] may be seen as part of a renewed interest in a coordinated approach to the regulation of digital and data-intensive technologies. This framework was recently further complemented with the AI Liability Directive proposal[12] and the revised Product Liability Directive proposal.[13]

The EC demonstrates profound awareness and an ambition of global leadership in setting up what could be termed as the new gold standard in the relationship of data with digital technologies, and the broader socio-economic effects connected to that. The new European Union (EU) gold standard frames this relationship around a set of core values that include a competitive and functioning single market (not surprisingly the legal basis of all these interventions) as well as fairness, proportionality, accountability, and transparency. This represents an important, yet not entirely new, feature of the legislation here discussed: the explicit inclusion in the regulatory framework of data of relevant EU Charter's fundamental rights. Illustratively, personal data and the privacy of communications,

[1] Doctoral researcher at Centre for IT & IP Law (CiTiP), KU Leuven, Belgium.

[2] Research Professor of Intellectual Property Law, Centre for IT & IP Law (CiTiP), Faculty of Law and Criminology, KU Leuven.

[3] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) [2022], OJ L 152/1.

[4] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information [2019], OJ L 172/56.

[5] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union [2019], OJ L 303/59.

[6] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A European strategy for data (the European Data Strategy), COM/2020/66 final [2020].

[7] Commission, 'Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC' COM/2020/825 final (DSA proposal).

[8] A final version of the DMA was agreed upon by the European Parliament and the Council on 12 May 2022, see Regulation (EU) 2022/… of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), 2020/0374 (COD).

[9] Commission, 'Proposal from the European Commission for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act or AI Act) and amending certain union legislative acts' [2021], COM/2021/206 final.

[10] Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (Directive on Copyright in the Digital Single Market) [2019], OJ L 130.

[11] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation or GDPR) [2016], OJ L 119/1.

[12] Commission, 'Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive)' [2022] COM (2022) 496 final

[13] Commission, 'Proposal from the European Commission for a Directive of the European Parliament and of the Council on liability for defective products (revised Product Liability Directive proposal or revised PLD proposal)' [2022] COM/2022/495 final.

intellectual property rights, consumer protection, the right to use and dispose of lawfully acquired possessions, the rights of children as vulnerable consumers, the freedom to conduct a business and the freedom of contract, as well as fair and effective protection against unfair contractual terms are all specifically identified in the Data Act Proposal Impact Assessment.[14] The resulting framework may be represented as a model of governance in between pure market dynamics and a fully regulated environment, combining elements that traditionally belong to private law and public law domains.

Within the above outlined framework, the Data Act proposal purports to enable and to promote the creation of value from data, especially privately held data, clarifying entitlements, conditions, and procedures along three main types of interactions: Business to Consumers (B2C), Business to Business (B2B) and Business to Government (B2G). This is done following two main legislative methods. First, the EC purports to fix several data-related issues such as data-driven foreclosures of markets and abuse of dominance in the field of IoT products as well as cloud and edge computing, therefore focusing essentially on B2B interactions. Second, the Data Act proposal intends to advance a political project for the European data economy to create more value and innovation from data exchange and re-use, here focusing on all three types of interactions. As we will see, this second approach reveals one of the most ambitious undertakings of the EC Data Strategy: the realisation of European Data Spaces.

To achieve these strategic results (competition, value creation, fair data exchanges and innovation), despite some initial demands in the opposite sense, the chosen way has not been that of a property-based approach, or in other words the creation or the extension of (intellectual-) property rights to IoT data. This is another crucial element of the EU data strategy. The EU has long had an infatuation towards the recognition of property or quasi-property rights in data. Illustrative is the (almost exclusively European) Sui Generis Database Right (SGDR) that, by protecting certain databases, offers a degree of property-based protection to the data therein contained.

During the drafting phase of the Data Act, among the various options considered to incentivise the opening-up of privately held databases, an extension of the current SGDR to machine-generated data or the ex-novo creation of a new property right in machine-generated data were taken into consideration, along with other non-property approaches (for example, a specific unfair competition remedy somehow similar to the one adopted in Japan).[15] The rejection of this proprietary approach as an incentive to disclose and exchange data (a kind of bargain theory common for instance in the field of patent law) in favour of the creation of a set of access and portability rules, combined with provisions regulating B2B and B2G data exchanges – or, in other words, the adoption of a data governance instead of a data property approach – is another central characteristic of the EU data strategy. [16]

Nevertheless, the question of how to reach and unleash the value contained in privately held databases remains. In fact, whereas the Open Data Directive (ODD) enacts a set of rules on the reusability of High Value Datasets as well as of research data and data held by Public Sector Bodies (PSBs), and whereas the DGA extends those approaches – in the form of recommendations – to data

[14] See, for example, Commission, Commission Staff Working Document 'Impact Assessment Report' accompanying the document Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act) SWD (2022) 34 final, sec 3 (end of section).

[15] Tatsuhiro Ueno, 'Chapter 6: Big data in Japan: Copyright, trade secret and new regime in 2018' In Sharon K. Sandeen, Christoph Rademacher, and Ansgar Ohly (eds), *Research Handbook on Information Law and Governance* (Cheltenham, UK: Edward Elgar Publishing, 2021)

[16] Thomas Margoni, Martin Kretschmer, 'A Deeper Look into the EU Text and Data Mining Exceptions: Harmonisation, Data Ownership, and the Future of Technology' (2022) 71(8) GRUR International, 685<https://academic.oup.com/grurint/article/71/8/685/6650009> accessed 13 October 2022.

held by PSBs that are excluded from the ODD, a similar approach, albeit conceivable, would have been difficult to implement for privately owned databases. This would have necessarily taken the form of some sort of positive obligation to make available privately held databases, with the potential to encroach upon property, trade secrets, and competition principles.

The road chosen by the EU is innovative, inspired, far-reaching and takes the name of European Data Spaces. In other words, the creation of a mixed public-private regulatory space will offer the infrastructural and regulatory framework within which data, including privately held datasets, will be voluntarily, or mandatorily when the required, exchanged for economic and societal benefit. This will effectively become what has been termed the European single market for data. By doing so, the EC aims to foster data sharing and re-use, which is expected to deliver growth and innovation, to support policy making and to preserve European values such as privacy, property, competition, consumer protection, pluralisms, safety, security, fairness, ethical standards and digital sovereignty. [17] This body of law, or acquis Communautaire following EU parlance, is increasingly viewed as 'data regulation' or, perhaps more academically, the nascent field of EU Data Law.

## 1.2 Overview of the Data Act proposal: Policy objectives

The considerations discussed above in abstract terms translate into the distinct chapters of the Data Act. Each chapter aims to fulfil specific objectives, as stated by the EC in its Explanatory Memorandum. This section offers a brief overview of the core objectives and corresponding chapters.

a) *"Facilitate access to and use of data by consumers and businesses, while preserving incentives to invest in ways of generating value through data"*

This objective is operationalised in Chapters II to IV (chapter I elucidates subject matter, scope and definitions). Chapter II lays down rules concerning access and use of IoT products' data (B2B and B2C data sharing). The stated goal is to empower IoT product users vis-à-vis IoT product manufacturers (also known as 'data holders') with respect to such data. Chapter III is constructed as a general regulatory framework applicable to data holders legally obliged to make data available. A clear – yet implicit – connection with upcoming European Data Spaces, for which more specific data sharing obligations may be adopted (such as in the case of the European Health Data Space Regulation) is palpable. Finally, Chapter IV aims to articulate the principle of fairness in B2B commercial data transactions, although this is only to the benefit of small and medium-sized enterprises (SMEs).

b) *"Provide for the use by public sector bodies and Union institutions, agencies or bodies of data held by enterprises in certain situations where there is an exceptional data need"*

Such objective relates to Chapter V, which aims to allow public sector bodies to require access to data held by the private sector (B2G data sharing) to address situations of so called 'exceptional needs', which plausibly cover emergencies such as the Covid pandemic.

c) *"Facilitate switching between cloud and edge services" ('data processing services')*

Chapter VI aims to addresses some enduring lock-in vendor issues in cloud computing, which were left unsolved by the 2018 Free-Flow of Non-Personal Data Regulation.[18] With carefully selected words, the latter Regulation laid down an 'encouragement' for cloud computing service providers to develop self-

[17] On Data Spaces, see Commission Staff Working Document on Common European Data Spaces, SWD (2022) 45 final.

[18] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union [2018] OJ L 303/59 (Free-Flow of Non-Personal Data Regulation).

regulatory codes of conduct expected, in turn, to 'facilitate' the switching of service providers and the porting of data from one to the other.[19] With the Data Act proposal, the EC engages much more decidedly with a detailed set of rules which effectively amount to a 'right to switching'.

d) *"Put in place safeguards against unlawful data transfer without notification by cloud service providers"*

This objective forms part of the broader digital sovereignty strategy of the European Union.[20] The 'safeguards' and more generally the regulation of international data transfer by data processing service providers, are regulated as per Chapter VII.

e) *"Provide for the development of interoperability standards for data to be reused between sectors"*

In this respect, Chapter VIII lays down an ambitious framework for further European Commission regulatory interventions concerning data (services) interoperability. Interoperability speaks directly to the needs and operations of European Data Spaces.

f) *"Enforcement"*

Chapter IX requires Member States to establish yet again 'competent authorities' to ensure the application and enforcement of the Data Act substantive provisions, with the additional objective to ensure consistency between the various data-related legal frameworks.

g) "*Clarifications relating the Sui Generis Database Right and IoT generated data*"

Finally, the short Chapter X intends to clarify the scope of the SGDR in relation to IoT generated data as defined and regulated in Chapter II.

In summary, the proposed measures constitute an ambitious and insightful but also complex framework for the regulation of data flows, which are expected to have a profound impact on the EU legal order and beyond.

## 1.3 Analysis of the Data Act Proposal: Overall structure

The Data Act Proposal addresses a complex and heterogeneous set of issues related to the data economy, following different approaches depending on the specific area of regulation. Here we offer an overview where we attempt a classification of the various initiatives in function of their specific goals: i) Fixing well-known issue in data markets: A pragmatic approach; ii) Unleashing the value of privately held data: Data Spaces; iii) Innovative approaches: data in the public interest, data sharing and data co-generation; iv) Regulatory interfaces: The Data Act and information law.

### 1.3.1 Fixing well-known issues in data markets: A pragmatic approach

**Business to Business data contracts.** The regulation of B2B data contracts in Chapter IV follows a pattern increasingly visible in recent EU legislation. According to this pattern, B2B contracts are becoming regulated through the lenses of commercial fairness. Whereas B2C unfair commercial practices have been subject to full-fledged EU horizontal and largely sector-agnostic regulation for a

[19] Free-Flow of Non-Personal Data Regulation, art 6.
[20] See, for example, the European Data Strategy, sec 6.

long time, it is only recently that B2B contracts have been the object of direct EU legislative attention.[21] This recent legislative and policy thoughtfulness seems certainly on the rise as witnessed by an ample regulatory activity. Illustratively, in 2019, the European Union legislator adopted a Directive on unfair trading practices in B2B relationships in the agricultural and food supply chain[22] as well as a Regulation on the relationships between online platforms and their business users,[23] the goals of latter Regulation being developed further by the DMA. Chapter IV of the Data Act proposal contributes to this growing attempt to regulate B2B unfair commercial practices, with the focus being placed, this time, on the object of contracts (namely data) and on the type of businesses, as it only applies to contracts imposed on SMEs. When Chapter IV is read in combination with Chapter II (the regulation of IoT data), it can be noted how, when both apply, they essentially create a new framework for data contracts, subject to the 'fairness test' of Chapter IV.[24]

**Non-personal data portability.** Chapter VI's evident aim is to address the gaps left by the soft law approach embraced in the Free-Flow of Non-Personal Data Regulation concerning the well-known issue of cloud computing vendor lock-in.[25] The correlation between the two initiatives appears evident when considering the power attributed to European standardisation bodies to deal with interoperability issues in cloud computing switching. The lack of interoperable standards has indeed emerged as the main hurdle preventing service providers' adoption of effective self-regulatory 'Codes of Conduct' pursuant to the Free-Flow of Non-Personal Data Regulation. This is a laudable initiative; however, as it will be discussed in the relevant sections,[26] Chapter VI is not immune from a certain degree of conceptual and terminological inconsistency. On the other hand, Chapter VI perfectly illustrate how the portability of data – which since its original delimitation to personal data has now developed into an almost general data portability principle – has become a popular legal mechanism to deal with data-related market failures, and especially vendor lock-in issues. This is not only the case with cloud and edge computing as per Chapter VI[27] but also with IoT data as per Chapter II.[28] Concerning health data, this can be seen in the dedicated Health Data Space Regulation proposal.[29]

**International non-personal data transfers.** The regulation of international non-personal data transfers by cloud and edge service providers aims to feed the digital sovereignty policy agenda of the EU.[30] It not only complements the legal regime of international transfers of non-personal data under the DGA, but also that of personal data under the GDPR and can thus be viewed as their ideal continuation. This being the case, the issue of effectively distinguishing between personal vs non-personal data and their dedicated legal regimes which often coexist within the same datasets, raises feasibility questions.[31]

[21] With the exception of Directive 2006/114/EC of the European Parliament and of the Council of 12 December 2006 concerning misleading and comparative advertising [2006] OJ L 376/21.

[22] Directive (EU) 2019/633 of the European Parliament and of the Council of 17 April 2019 on unfair trading practices in business-to-business relationships in the agricultural and food supply chain [2019] OJ L 111/59.

[23] Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services [2019] OJ L 186/57.

[24] See sec 6.

[25] Data Act Impact Assessment n11, Annex 9.

[26] See, for example, sec 10.

[27] See sec 10.

[28] See secs 2-3.

[29] See sec 3.

[30] See Tambiama Madiega, 'Digital sovereignty for Europe' (2020) EPRS Ideas Paper: Towards a more resilient EU <https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf> accessed 12 October 2022.

[31] See secs 11-12.

**Competent authorities.** The identification of 'competent authorities' empowered to enforce the provisions of the Data Act also follows a path often travelled. The appointment of 'competent authorities', 'regulatory bodies', 'dispute-resolution bodies' or otherwise called administrative authorities to supervise the application of a given piece of legislation, has become a common element of EU law in the last three decades. This phenomenon is thus neither new nor specific to the digital environment. What appears novel, however, is the growing overlap of the respective competence of such bodies, which is particularly visible when dealing with 'data' as the main object of legal entitlements and/or transactions. Because of their abstract nature and terminological vagueness, data often find themselves amid various concurrent legal frameworks. As the Data Act thereby adds a new legislative layer to legacy legal frameworks, an increasing number of administrative bodies have concurrent jurisdiction on data processing activities leading to different – and potentially contradictory – determinations, as discussed in Sec. 13.

### 1.3.2 Unleashing the value of privately held data: Data Spaces

The Data Act proposal can be viewed as the end point of two major tensions in the data economy policy. The first tension lies between the ambition to create a unique single market for data, on the one hand, and the needs emerging from sector-specific idiosyncrasies in data markets, on the other. In regulatory terms, this translates into a question of whether data should be regulated horizontally or rather in a sector-specific and vertical manner (for example, by developing specific rules for data markets in the agricultural, mobility, health, circular economy, etc., sectors). Naturally, the more sector specific regulations there are the less generalizable (read: interoperable) sector specific data spaces will be, compromising the overall goal of a single market for data. The second tension is specific to private sector data, which are arguably the most numerous and possibly valuable ones. The tension lies in between the goal to foster data re-use on a large scale, on the one hand, while not drifting into a heavy top-down regulation of privately held datasets, for instance by imposing positive obligations to disclose, on the other.[32]

The theory of data spaces appears to constitute the way out to both tensions. In its European Data Strategy of 2020, the EC opted for a two-tiered approach, whereby horizontal rules would be complemented by (sector- or domain-) specific ones when necessary.[33] Sector-specific regulation will be structured around the notion of sectorial data spaces, with nine initial data spaces being originally identified under the European Data Strategy and more to follow. For some of them, specific EU regulations will be adopted (and/or have already been proposed in the case of the Health Data Space), to foster standardisation and interoperability, as well as to set data access rights and provide for specific governance mechanisms. The very notion of 'data spaces' remains partially undefined and, strangely enough, not outlined neither in the DGA or in the Data Act proposal. This is all the more unexpected considering that 'operators of data spaces' have interoperability obligations under the Data Act.[34]

---

[32] Such a drift has been identified as a risk in certain sectoral legislations. It was made conceptually possible by the (implicit) idea of data as a 'purposive infrastructure' for the data economy, sometimes confused with a competition law purpose for imposing data sharing obligations, Charlotte Ducuing, 'Data as Infrastructure? A Study of Data Sharing Legal Regimes', *Competition and Regulation in Network Industries*, 23 December 2019, https://doi.org/10.1177/1783591719895390.

[33] Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: "A European strategy for data" COM(2020) 66 final

[34] 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 ('Data Act proposal'), art 28(1).

The Data Strategy refers, generally, to a 'single European data space' as

> a genuine single market for data, open to data from across the world – where personal as well as non-personal data, including sensitive business data, are secure and businesses also have easy access to an almost infinite amount of high-quality industrial data, boosting growth and creating value, while minimising the human carbon and environmental footprint.[35]

The Commission Staff Working Document on data spaces provides a more practical and workable vision of data spaces. Data spaces are designed to overcome

> legal and technical barriers to data sharing by combining the necessary tools and infrastructures and addressing issues of trust by way of common rules. A common European data space brings together relevant data infrastructures and governance frameworks in order to facilitate data pooling and sharing.[36]

Data spaces shall include

> "(i) the deployment of data sharing tools and services for the pooling, processing and sharing of data by an open number of organisations, as well as the federation of energy-efficient and trustworthy cloud capacities and related services", (ii) data governance structures […]" and they will aim at "(iii) improving the availability, quality and interoperability of data […]".[37]

Such a definition would seem to imply that both the nature and boundaries of data spaces may differ from one another, for instance in function of the sector or industrial partners. In any case, the definition suggests noticeable differences compared to the early sources of the concept of 'data space' in the engineering literature.[38] In any case, it is clear that, in the eye of the EC, data spaces shall be supported by legislation where appropriate but shall not be unduly constrained by it.

An important, perhaps unique, feature of the novel EU Data Law approach is the creation of a set of horizontal rules that will apply to all data spaces, irrespective of the specific sector. It is under this light that the Data Act and the DGA can be seen in all their regulatory splendour. Not only regulation of several types of data intermediaries, but also IoT data regulation under Chapter II Data Act is to be considered 'horizontal' in the sense that it applies to IoT data irrespective of the sector. Similarly, B2G data sharing under Chapter V Data Act is also sector-agnostic. Additionally, the Data Act lays the basic legal infrastructure for data spaces with both Chapter VIII, which creates the legal basis for the EC to adopt interoperability standards, and Chapter III, which sets the general legal conditions applicable upon mandatory making available of data.

---

[35] Commission, 'Communication "A European Strategy for Data"', COM/2020/66 final § (2020), sec. 3, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066.

[36] Commission Staff Working Document on Common European Data Spaces, SWD (2022) 45 final, 2.

[37] Commission Staff Working Document on Common European Data Spaces, SWD (2022) 45 final, 23.2.2022, Section 2.

[38] In the original definition of GAIA-X, indeed, data spaces were viewed mainly from a technological perspective whereby the main focus is placed on the decentralisation of data storage (at data source) and data standards, seemingly viewed as a (sufficient) guarantee for fairness and trustworthiness, Gaia-X <https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html> accessed 7 October 2022. See also Boris Otto and Matthias Jarke, 'Designing a multi-sided data platform: findings from the International Data Spaces case' (2019) 29 Electron Markets, 561. For a literature review on the notion of 'data space', see Edward Curry, Simon Scerri, and Tuomo Tuikka, Data Spaces: Design, Deployment, and Future Directions, in *Data Spaces Design, Deployment and Future Directions*, eds. E. Curry, S. Scerri and T. Tuikka, Springer, 2022.

In anticipation of sector- and/or data space-specific regulation, Chapter III provides, indeed, that any data holder mandated to make data available to (a) data recipient(s) shall do so transparently and following 'fair, reasonable and non-discriminatory' (FRAND) terms.[39] Lex specialis regulation – that is, data space-specific regulation – may depart from Chapter III, although seemingly only where more stringent on the data holder.

The provisions here discussed perfectly illustrate the tension between horizontal vs sector-specific regulation of data and the approaches developed by the EC to tackle it. The EC demonstrably aims to alleviate obstacles to the emergence of 'fair' data markets in all sectors and, insofar as possible, cross-sectors. The expectation with FRAND terms applicable virtually to any data sharing obligations in various sectors, is that they constitute both a unique yardstick while being flexible enough to allow for (sectoral) specificities in their application.[40]

Finally, Chapter VIII lays down extensive provisions for the regulation of interoperability for data spaces to operate, among other things. Interoperability shall be present at the level of data, data sharing (including the technical means to do so) and smart contracts when used to automate data transactions.[41] The EC may further substantiate essential requirements. European standardisation organisations will likely play a key role to elaborate harmonised standards, the compliance with which grants to operators of data spaces a presumption of conformity with the essential requirements.[42] Interoperability – and standardisation as a means to achieve it – is well-known to be essential to the advent of a genuine single market for data. The elaboration of essential requirements and of standards will thus constitute the birth certificate of data spaces. Given both the amount of data spaces and the scope of interoperability under Chapter VIII of the Data Act, it remains to be seen how the EC and the standardisation organisations will keep pace.

### 1.3.3 Innovative approaches: data in the public interest, data sharing and data co-generation

Although designed to tackle well-known issues concerning data access and sharing in the EU, some provisions of the Data Act proposal are truly innovative and global.

Arguments have long been raised that data held by the private sector could support governments in policymaking and, more generally, public sector bodies in the conduct of their public service activities.[43] The question is immense and runs through sectors, disciplines and markets. Illustratively, consider the examples of how product-related data held by manufacturers are necessary to design indicators on the transition to a circular economy, or of how the Covid pandemic showed very

[39] Data Act proposal, art 8(1).

[40] This is also the view held by Habich in 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) IIC <https://doi.org/10.1007/s40319-022-01255-x> accessed 18 October 2022. Picht talks about a "magical incantation". Peter Georg Picht, 'Caught in the Acts: Framing Mandatory Data Access Transactions under the Data Act, further EU Digital Regulation Acts, and Competition Law' (2022) Max Planck Institute for Innovation and Competition Research Paper No. 22-12, 41 < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4076842> accessed 18 October 2022. On the matter, see also sec 4.

[41] Data Act proposal, art 28(1) and art 30.

[42] ibid, art 28(3) and (4).

[43] See Commission, Directorate-General for Communications Networks, Content and Technology, 'Towards a European strategy on business-to-government data sharing for the public interest: final report prepared by the High-Level Expert Group on Business-to-Government Data Sharing' (2021) <https://op.europa.eu/en/publication-detail/-/publication/d96edc29-70fd-11eb-9ac9-01aa75ed71a1> accessed 12 October 2022.

concretely the extent to which data held by diverse private entities may help public sector bodies in tackling extraordinary catastrophes. Likewise, data may serve to fight climate change in different manners and at different scales. Many concepts have been coined with a view to finding the right balance between the pursuit of the general interest for accessing and using data while preserving the legitimate interests of private sector bodies to retain them, such as 'private data of general interest',[44] 'reference data',[45] 'data for the common good',[46] and 'civic (or public) data trust'.[47] The discussion is also closely connected to data philanthropy, which has eventually crystallised in the form of 'data altruism' in the DGA.[48] Additionally, the Data Act proposal introduces the concept of 'exceptional needs' under which public sector bodies can request privately sector data, albeit under strict conditions. On this basis, chapter V provides for a general and ambitious B2G data sharing legal framework.

The questions raised by the absence of a legal statute of IoT data are also well-known and are usually framed as follows. IoT products are tangible devices with built-in sensors and software which generate, process and communicate data while being operated (such as about their environment), for instance smart tractors, fridges or watches. Such data may notably improve the devices' operation to the benefit of the user or be further aggregated and processed by the manufacturer to gain insights on users' activities and, hence, optimise products and services' offering. Questions arise as for who, amongst them, should be entitled to the data use and value. Although generated by the interactions of several stakeholders, data stemming from IoT products are often appropriated by IoT product manufacturers or providers of related services (in the parlance of the EC) who reserve the exclusive access to and use of such data to the detriment of product users, whether consumers or businesses, but also of competitors in aftermarkets and consequently of innovation. It is against this background that, already in 2016, the EC laid down the option to create a form of data ownership to empower users (the 'data producer's right), accompanied by data sharing obligations.[49] A policy and scholar consensus formed against the institution of data ownership which was eventually abandoned.

---

[44] See, for example, Commission, 'Urban Agenda for the EU: Digital transition action plan' (2018) final <https://ec.europa.eu/futurium/en/system/files/ged/digital_transition_action_plan_for_dgum_300818_final.pdf> accessed 12 October 2022.

[45] According to the EU Vocabularies: ' Reference data, such as code lists and authority tables, means data that are used to characterise or relate to other data. Such a controlled vocabulary defines the permissible values to be used in a specific field for example as metadata. Reference data vocabularies are fundamental building blocks of most information systems. Using common interoperable reference data is essential for achieving interoperability.' Publications Office of the European Union, 'EU Vocabularies' <https://op.europa.eu/en/web/eu-vocabularies/semantic-knowledge-base> accessed 12 October 2022.

[46] See Commission Staff Working Document Impact Assessment Report Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on European Data Governance (Data Governance Act) SWD/2020/295 final.

[47] See European Parliamentary Research Service, Joan Lopez Solano, Aaron Martin, Siddharth de Souza and Linnet Taylor, 'Governing data and artificial intelligence for all: Models for sustainable and just data governance' (2022) <https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729533/EPRS_STU(2022)729533_EN.pdf> accessed 12 October 2022.

[48] See Commission, 'Impact Assessment on enhancing the use of data in Europe, Report on Task 1 – Data governance' (2019) Smart 2019/0024 | D2 <https://digital-strategy.ec.europa.eu/en/library/impact-assessment-report-and-support-study-accompanying-proposal-regulation-data-governance> accessed 12 October 2022. See also See Commission, Directorate-General for Communications Networks, Content and Technology, 'Towards a European strategy on business-to-government data sharing for the public interest: final report prepared by the High-Level Expert Group on Business-to-Government Data Sharing' (2021) <https://op.europa.eu/en/publication-detail/-/publication/d96edc29-70fd-11eb-9ac9-01aa75ed71a1> accessed 12 October 2022.

[49] Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: "Building a European Data Economy"' COM(2017) 9 final European

In turn, several sectoral data sharing legal regimes have been adopted. The question then arose how to proceed further, whether from a purely sectoral perspective or based on horizontal regulation, whether based on public law (that is, based on competition law(-inspired) data sharing obligations)[50] or private law premises (based on the bundle of property rights approach, or through the regulation of unfair commercial terms). The American Law Institute ('ALI') and the European Law Institute ('ELI') proposed a framework for the creation of 'data rights', which can be seen as a synthesis of the debates.[51] Based on both private and public law considerations, the ALI-ELI Principles for a Data Economy also undertake to bridge the gap with the GDPR, conceived of as a materialisation of 'data rights' granted to data subjects for privacy reasons, while other 'data rights' could be granted to the same or other stakeholders for other reasons, such as allocating data use and restoring competition.

With the Data Act proposal, the EC is visibly influenced by the ALI-ELI Principles. Not only does Chapter II grant access rights to co-generated data to users, but it also governs the use of data by the three categories of actors (triangular relationship) at stake, namely the data holder (often the manufacturer), the users and the 'third party' that the users can entrust with their data. The regulation of IoT data proposed by the EC constitutes a major innovation. Beyond access rights, the proposal also regulates the use of data by the parties in the triangle and attempts to find an obviously delicate ridgeline between the empowerment of users (for example, right to repair), the protection of data holders' investments (through the protection of trade secrets) and the promotion of competition (transferability of data to third parties).

### 1.3.4 Regulatory interfaces: The Data Act and other areas of information law

As common in this type of legislation, third party rights, especially when they can be linked to the broader category of property rights, remain largely untouched. This is the case with intellectual property rights and the Data Act.[52] Two exceptions are however noteworthy: Trade secrets (TS) and the Sui Generis Database Right (SGDR).

Sec. 15 discusses the relationship between the Data Act and the Trade Secret Directive.[53] This is a complex relationship, especially in relation to the often too abstract distinction between raw data (frequently devoid of trade secrecy) and derived information (a much more familiar category for TS). The notion of 'disclosure' regulated in unexpected ways in the Data Act is likewise in need of attention. Finally, the possibility that data holders may act, essentially, as regulatory agents for the identification and protection of their own trade secrets, with the ensuing risk of trumping their own data sharing obligations is another aspect that needs proper consideration.

As indicated above, the Data Act has rejected a proprietary approach to the regulation of data. In fact, it not only did not include a new data producer right, but it even elucidated that the current SGDR does

Commission, 'Communication Building a European Data Economy', 2017; European Commission, 'Commission Staff Working Document on the Free Flow of Data and Emerging Issues of the European Data Economy - Accompanying the Document "Communication Building a European Data Economy"', 2017.

[50] See, for example, Act to Strengthen Consumer Protection in Competition and Trade Law (Federal Law Gazette Part I n. 53, 17 August 2021)(Germany).

[51] ALI-ELI, 'Principles for a Data Economy' (American Law Institute - European Law Institute, 2020), https://www.europeanlawinstitute.eu/projects-publications/current-projects-feasibility-studies-and-other-activities/current-projects/data-economy/.

[52] See 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 (Data Act proposal), just after fn 20, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A68%3AFIN#footnoteref20; Data Act proposal, rec 28.

[53] Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure [2016] OJ L 157/1.

not apply to IoT data. Article 35 of the Data Act indeed 'clarifies' that the SGDR does not apply to databases containing data obtained from or generated by IoT products or related services. However, this framing of the issue only reiterates the longstanding debate on the creation (now generation?) v obtaining of data, especially when the data is observed or recorded from the surrounding environment, as arguably it is the case in many IoT situations. Sec. 14 assess the current formulation of Article 35 and indicates possible drafting options.

Technical protection measures constitute a well-known interaction between legal- and techno-regulations, whereby technology is used to enforce legal rights or occasionally power asymmetries. The Data Act addresses the use of 'Technical protection measures' (TPMs) deployed by data holders. As discussed in Sec. 5, whether legal rights and entitlements on the one hand, and TPMs on the other, are fully aligned remains disputed. Furthermore, Technical Protections Measures under Article 11 of the Data Act and Technological Protection Measures under EU Copyright Law, may or may not share a common legal denominator. More clarity in this area seems essential given the relevance of technological solutions in the realisation of European Data Spaces.

It seems largely self-evident that, when converging on the same subject matter, data sharing obligations may be in sharp contrast with the protection of personal data, especially as regulated in the GDPR. The latter is indeed based on core principles such as data minimisation and purpose limitations, which means that the very collection of data, qualified as a form of 'data processing' should itself be motivated by a legitimate purpose, subject to a necessity and proportionality test. The tensions between the Data Act and personal data protection are many. There is a risk that, the Data Act message may be interpreted as a "move in practice from a strict necessity test for personal data processing to an appropriateness or acceptability of processing paradigm" which, it is argued, is "a bleak scenario for our privacy".[54] The impact of the Data Act on privacy and personal data protection is discussed further in Sec. 3 where the 'individuals' empowerment' motto of data portability is critically assessed. Sec. 9 further discusses the privacy and personal data protection implications of the B2G data sharing obligations under Chapter V of the Data Act. Enforcement, and in particular the role of data protection authorities ('DPAs'), will play a key role in ensuring a sound balance between data sharing and the protection of individuals. In this context, Sec. 13 identifies a risk under Chapter IV of the Data Act concerning both the independence and role of DPAs.

Finally, Sec. 16 offers a novel analysis of the interaction between the Data Act and cybersecurity regulations, based on the analysis of medical devices as a case study. Cybersecurity should obviously play a significant role in the future design of essential requirements and standards, following Chapter VIII of the Data Act, which should thus be further scrutinised. The Data Act proposal is evidently designed to complement the newly adopted DGA. The DGA regulates intermediaries (understood in the broader sense) in order to bring trust to data holders and (re)users when exchanging data in various situations (for example, commercial or non-commercial, private or public sector data, etc). The DGA is therefore expected to constitute a major building block for data exchange to take place in the EU. The Data Act and the DGA share a few similarities, especially in terms of cornerstone notions. For instance, they rely on the same (broad) definition of 'data'[55] and they both endorse the distinction between

[54] Jan Czarnocki, 'Data Act Message – Legitimacy of the Data Processing and Consistency of Data Protection' (*CiTiP Blog*, 3 May 2022) <https://www.law.kuleuven.be/citip/blog/data-act-message-legitimacy-of-the-data-processing-and-consistency-of-data-protection/>.

[55] DGA, art 2(1); Data Act proposal, art 2(1).

'personal' and 'non-personal' data.[56] That said, the key definition of 'data holders' diverges in the DGA and in the Data Act proposal, arguably on grounds of the specificities of the respective regulations.

The DGA provides for a trust infrastructure for actors to rely on when exchanging data. In contrast, the Data Act consists mainly in obligations to make data available in different scenarios, often on the basis of fairness considerations. There should be sharp interfaces between the two regulations, which are however not clearly anticipated by the Data Act. For example, as already highlighted, it remains unclear how data intermediaries within the meaning of Chapter III of the DGA could support users in making further use of their IoT data. [57]

In terms of enforcement, both the DGA and the Data Act require the establishment of 'competent bodies', which will inevitably have to cooperate with already established enforcement authorities. It remains to be seen concretely how Member States will operationalise enforcement and, in particular, how they will deal with the need for cooperation.[58]

Finally, the Data Act places a strong emphasis on the regulation of specific types of contracts, such as 'data processing services' (that is, cloud computing) under Chapter VII and data access and use contracts (or contractual stipulations as part of broader contractual relationships). Sec. 6 analyses this phenomenon concerning the relationship between the data holder and the data recipient to whom the data holder is requested to make data available (Chapter III of the Data Act). Sec. 2 analyses a similar situation concerning the relationship between the data holder and the user under Chapter II of the Data Act and identifies several questions including how the regulation of 'switching' between data processing service providers under Chapter VII interacts with the Digital Content Directive.

## 1.4 Final considerations

In the above we have attempted an initial classification of the Data Act following a functional perspective and thus trying to match the specific goals of the broader EU Data Strategy and the specific methods or approaches followed in the Data Act to achieve them. This is a helpful exercise in order to maintain a high-level understanding of the direction in which data regulation is evolving. In the next section a detailed analysis of each section, chapter or topic of the Data Act will illustrate further the current state of play in the field of data law.

[56] DGA, art 2(4); The Data Act proposal does not define 'non-personal data' but lays down provisions which apply specifically to such data, see for example art 4(6).

[57] Picht (n 41) 30-32; Peter Georg Picht and Heiko Richter, 'EU Digital Regulation 2022: Data Desiderata' (2022) 71(5) GRUR International, 395, 398.

[58] See sec 13.

## 2 Chapter II of the Data Act – Data control of users – Charlotte Ducuing[59]

Chapter 2 of the Data Act consists mainly of a set of Internet-of-Things ('IoT') product data access and sharing (including portability) provisions. The main beneficiary is the product 'user', defined as "a natural or legal person that owns, rents or leases a product or receives a service".[60] Essentially, the user of an IoT product or related service, whether a legal or natural person, may require from the 'data holder' – most often, the manufacturer or operator of related service(s) - access to the data generated by the use of the product where such data are not already made accessible 'by design'. Further, the user is entitled to share – and have ported – such data to a third party for the purpose defined by the user, except to develop competing products, among other things. The provision builds on the precedent of the data portability right afforded to data subjects by the GDPR,[61] as discussed further in sec. 3 of this White Paper. The Data Act governs the typical blind spots left unsolved by the data portability right under the GDPR, such as the conditions requested by the data holder for the operationalisation of the porting and the limitations to data use by the third party.[62] Importantly, real-time data are in the scope 'where applicable'. In principle, Chapter 2 applies to both 'personal' and 'non-personal data'.

Both data access and sharing rights have been high on the EU political agenda for a few years now.[63] The Data Act proposal builds on both the GDPR and previous data access sectoral legislation.[64] By doing so, the EC aims, first, to restore balance between 'data holders' and users, whether individuals or (small) companies. The latter are indeed often prevented from using data they contribute to generating while the use of data by data holders may be detrimental to them. Second and relatedly, user empowerment - or data control - is viewed as instrumental to fostering data reuse, thereby fixing market failures and creating innovation.[65]

This section takes stock of the EC's expectation to empower users with their data, which materialises in the proposal with two complementary facets. With the 'defensive' or 'negative' facet, the proposal protects the user against the likelihood of harm associated with the processing of data, in particular from the data holder. With the 'active' or 'positive' facet, the proposal provides users with tools so they can make genuine use of 'their' data.[66] In this context, selected items concerning both facets are

[59] Doctoral researcher at Centre for IT & IP Law (CiTiP), KU Leuven, Belgium.

[60] 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 (Data Act proposal), art 2(5).

[61] GDPR, art 20.

[62] Data Act proposal, arts 5 and 6.

[63] This is for example visible throughout the European Data Strategy of the European Commission, 2020. Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: "A European strategy for data" COM(2020) 66 final.

[64] See for example, in the field of transport, Commission Delegated Regulation (EU) 2017/1926 of 31 May 2017 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the provision of EU-wide multimodal travel information services [2017] OJ L 272/1 (MMTIS); In the electricity sector, see Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU [2019] OJ L 158/125 (Electricity Directive).

[65] Data Act proposal, recs 6 and 14; see also the Commission, Commission Staff Working Document Impact Assessment Report accompanying the document Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act) SWD (2022) 34 final, 9-10, 26-27.

[66] This idea is further developed by the author in Charlotte Ducuing, 'An Analysis of IoT Data Regulation under the Data Act Proposal through Property Law Lenses' (2022) CiTiP Working Paper 2022, 26 <. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4225027> accessed 7 October 2022.

discussed so as to identify avenue for improvement, with a view to delivering on the data control policy ambition and on fairness more generally.

The question what 'data control' concretely means, whether a political buzzword, a risky path towards auto-exploitation of individuals[67] or a true way forward for the data economy, lies beyond the ambit of this section and calls for further analysis. The question whether data control, in general, can deliver on expectations is also not further discussed. More generally, this section does not provide an exhaustive assessment how the regulation of IoT data could be improved to empower users. In particular, two important aspects are not discussed: the scope rationae materiae, namely which data are governed,[68] and the question whether technology should be used to empower users while the Data Act proposal recognises TPMs to the benefit of data holders.[69]

## 2.1 The defensive facet of data control: Regulation of data holders' use of data

Not only are data holders mandated to share data, but their use of data is also regulated.[70] In particular, Article 4(6) lays down a two-tiered regulation of the use of non-personal data by the data holder, with the apparent assumption that the processing of personal data is sufficiently regulated under the GDPR.

### 2.1.1 Article 4(6), first sentence

First, the first sentence of Article 4(6) lays down a default ban on the use of non-personal data by the data holder, except when based on a contractual agreement with the user.[71] At first glance, this provision seems exceptionally restrictive on data holders. Even the GDPR does not deny processing but provides a list of possible legal basis for the processing of personal data.[72] In addition, the ban is hard to decipher and has already been discussed intensively.[73] A cause for unclarity lies with the notion of 'use', which is not defined in the proposal.

One interpretation could be that the provision bans non-personal data 'use' by the data holder, understood in the abstract, irrespective of the purpose and beneficiary, thereby endorsing a technical

[67] This refers to the critique of Robert Herian, 'Blockchain, GDPR, and Fantasies of Data Sovereignty' (2020) 12 Law, Innovation and Technology 156, 168.A similar critique is made to the Data Act, Beatriz Botero Arcila and Teodora Groza, 'Comments to the Data Act from the Law and Technology Group of Sciences Po Law School' (Sciences Po Paris, 2022), 2, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4135212. For an analysis of 'data control' as it manifests itself in the regulation of IoT data in the Data Act proposal, see Ducuing, 'An Analysis of IoT Data Regulation under the Data Act Proposal through Property Law Lenses'.

[68] On this, see, for example, Can Atik, 'Data Act: Legal Implications for the Digital Agriculture Sector' (2022) Tilburg Law School Research Paper, 8-10 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4144737> accessed 7 October 2022; Wolfgang Kerber, 'Governance of IoT Data: Why the EU Data Act will not Fulfill Its Objectives (second version) (2022) GRUR International, sec 4.2.2.

[69] On the topic of TPMs, see sec 5.

[70] See also the regulation of data use by the beneficiary of the data portability right, Data Act proposal, art 6.

[71] Article 4(6), first sentence, of the Data Act proposal states that "the data holder shall only use any non-personal data generated by the use of a product or related service on the basis of a contractual agreement with the user."

[72] GDPR, art 6.

[73] 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) https://pure.mpg.de/rest/items/item_3388757_4/component/file_3395639/content> accessed 7 October 2022, paras 44–55. As noted by the authors, the Data Act proposal does not clarify the legal consequences in case of breach, for example, for third parties holding such data in good faith.

interpretation. This interpretation could bring the notion of 'use' closer to this of 'processing', also referred to in the Data Act proposal. See for example in Article 6(1) concerning the regulation of data processing by the third party. The notion of 'processing' is defined, following the GDPR, as referring to

> any operation or set of operations which is performed on data or on sets of data in electronic format, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Following such an interpretation, the absence of a contractual agreement with the user would then theoretically result in no data being generated and, as a result, the remainder of IoT data regulation being simply watered down. Against this background, it seems fair to assume that this interpretation shall be discarded. Alternatively, 'use' could be granted a more legal meaning, in the sense of processing for one's own purpose(s). Article 4(6), first sentence, could then be read as allowing by default the processing of data by the data holder at the very least for the user's purposes, that is the operation of the product or service and the making available of data under Chapter II of the Data Act.

While the data holder – in its quality as manufacturer – is recognised as a co-generator of data,[74] the by default ban on use, irrespective of the interpretation, seems unfair and lacks a well-founded rationale.

This being, as a matter of fact, there is often a contract present between the data holder and the user that regulates data use. Because IoT product manufacturers are often in a stronger bargaining position, such contracts are currently often to the benefit of the data holder, who uses data for a broad range of (unrestricted) purposes.[75] As already highlighted, the remainder of the Data Act proposal assumes the existence of such contracts.[76] Although the vague expression 'contractual agreement with the user' will inevitably raise interpretation questions (for example, to the formation of a contract) before national enforcement authorities, it is plausible that, in most cases, data holders will retain the possibility to process data for their own purpose as a matter of fact.

### 2.1.2 Article 4(6), second sentence

The second sentence of Article 4(6) lays down another limitation, in the form of a purpose limitation, with respect to 'non-personal data': 'The data holder shall not use non-personal data to derive insights about the economic situation, assets and product methods of or the use by the user that could undermine the commercial position of the user in the markets in which the user is active'. Seemingly inspired by personal data protection legislation, such purpose limitation seems critical to prevent well-

[74] Data Act proposal, rec 6.

[75] Tommaso Fia, 'An Alternative to Data Ownership: Managing Access to Non-Personal Data through the Commons' 21(1) (2021) Global Jurist, 181 <https://doi.org/10.1515/gj-2020-0034>; Alain Strowel, 'Chapter 6: Big Data and Data Appropriation in the EU', in *Research Handbook on Intellectual Property and Digital Technologies*, Tanya Aplin, Research Handbooks in Intellectual Property Series (Edward Elgar Publishing, 2020), 113–14.

[76] Wolfgang Kerber, 'Governance of IoT Data: Why the EU Data Act will not Fulfill Its Objectives (second version)' (2022) GRUR International, 21-22 (forthcoming as third, revised version) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4080436> accessed 18 October 2022.

documented data-driven harm to be caused to (mainly business) users[77] and is thus a welcome step in the right direction.

This being, (business) users are well-known to fear the making available of data to third parties for lack of control on the downstream activities. However, it remains unclear to what extent Article 4(6), second sentence, protects them against this eventuality. The provision regulates the use of data by data holders and does not extend to the use of data by downstream recipients of data, to whom the data holders would have shared the data. Three aspects should be distinguished therein. First, Article 4(6), second sentence, lays down an obligation incumbent solely on the data holder and not on a downstream recipient. As a result, the user disposes of an enforceable right against the data holder, but not against the downstream data recipient (no direct action). Second, the reading of the provision seems to suggest that the data holder does not vouch for the use of data by a downstream recipient nor can it be held accountable for such use, should it be deemed illegitimate. Third, it remains unclear whether the sharing or transfer of the data by the data holder to a downstream recipient who would then engage into 'inferring insights' […] as laid down in Article 4(6), second sentence, consists in a violation of this provision by the data holder. This calls, again, into question the interpretation of the term 'use' (see above), namely whether the prohibited 'use' of the data by the data holder includes the sharing or transfer of such data to a downstream recipient or not. The Data Act proposal does not answer this question.[78] In any case, Article 4(6), second sentence, appears to provide a weak protection, if at all, against detrimental use of data by downstream recipients.

In turn, the Data Act proposal lays down transparency requirements pursuant to Article 3(2)(d), that are designed to protect the user against detrimental use of data, including by downstream recipients. Prior to the conclusion of a contract (assumingly regulating data use pursuant to Article 4(6), first sentence),[79] the data holder shall indeed provide the user with information on whether it 'intends to use the data itself or allow a third party to use the data and, if so, the purposes for which those data will be used' (emphasis added), among other things. This constitutes an evident improvement compared to the current situation. However, the legal value of such information (in other words, whether contractual or not) remains ambiguous, which renders legal consequences in case of violation unclear. Also, the notion of 'purpose' is undefined, so it remains to be seen to what extent it would enable users to ascertain concretely whether the purpose of use could be detrimental to them. Finally, this protection would then be, at best, of a contractual nature, which appears weak in view of the well-known unbalance of power and bargaining positions in many such markets (see above).

[77] Hummel and others conduct a philosophical analysis of the claims labelled as 'data ownership', where 'ownership' plays the role of a proxy for the problems encountered with data. They identify a need for protection against loss of control and related data-driven harm, see Patrik Hummel, Matthias Braun, and Peter Dabrock, 'Own Data? Ethical Reflections on Data Ownership' (2021) 34(3) Philosophy & Technology, 545 <https://doi.org/10.1007/s13347-020-00404-9> accessed 18 October 2022.

[78] Atik concludes that the Data Act proposal does not prevent data holders from sharing data to third parties, Can Atik, 'Data Act: Legal Implications for the Digital Agriculture Sector' (2022) TILEC Discussion Paper No. DP2022-013, 13–14 <.https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4172957> accessed 18 October 2022. However, his footnote 70 seems to suggest that Art. 5 of the Data Act proposal would address this problem, should it be clearly turned into a non-waivable provision. Our understanding is that Art. 5 deals with another issue, namely positive obligations for the data holder to share data rather than negative obligations not to share data.

[79] The reading of Recital 24 also confirms this interpretation: '[…] Any contractual term in the agreement stipulating that the data holder may use the data generated by the user […] should be transparent to the user, including as regards the purpose for which the data holder intends to use the data.'

## 2.2 The positive facet of data control: Do we need a tailored data portability right?

The Data Act proposal aims to empower users to make further use of their data, based on a sophisticated data portability right. This being, issues may arise in the practical implementation. In this subsection, we discuss two issues.

### 2.2.1 The data portability right: what about exhaustion?

First, whether the data portability right is subject to exhaustion or not remains a blind spot. It seems only logical that users may exert their right to data portability several times for different purposes and with respect to different third parties. This, however, is not clarified in the proposal. It should (and could easily) get fixed in the legislative process, in order to prevent refusals to deal by data holders on that ground.

### 2.2.2 The non-tackled issue of the sorting out of data in view of their further use

The second issue may be thornier. There is an evident misalignment between the data needed by the user and the chosen third party in a certain instance to fulfil an agreed purpose, and the data generated by an IoT product or related service. The nature of the data generated by IoT products or related services depends entirely on the business case of the manufacturer and/or provider and on the behaviour of the user and is therefore not harmonised and, to an appreciable extent, unexpectable to the chosen third party. In turn, the data needs depend on the given instance and purpose for which the data portability mechanism is exerted, and are thus specific. This raises the question how to align data demand and offer, in a given instance.[80]

The data holder benefits 'by design' information asymmetries that the Data Act laudably attempts to fix with transparency obligations, for example, concerning the nature and volume of data.[81] However, such obligations are (i.) to the benefit of the user and (ii.) they take place 'once and for all' prior to the conclusion of the contract with the user. They are thus not targeted at the specific needs of the chosen third party in a given instance and may not enable the chosen third party to know which data it can expect to receive, to the point that data may simply turn out to be inappropriate or insufficient.[82]

The Data Act proposal is also silent on the question how data should be sorted out in a given instance and by whom. The data holder may obviously prefer to sort data out prior to making them available to third parties in order to keep control of the data sharing process and to prevent the sharing of sensitive data (that is, trade secrets). This activity could be provided as a commercial service in exchange for compensation claimed to the third party.[83] However, it could result in both under-compliance and possibly in enabling the data holder to acquire sensitive knowledge on the business of the chosen third

[80] Kerber discusses also this issue and anticipates strategic behaviours from the data holder as a result, to try and narrow down the scope of data. Wolfgang Kerber, 'Governance of IoT Data: Why the EU Data Act will not Fulfill Its Objectives (second version) (2022) GRUR International, sec 4.

[81] Data Act proposal, art 3(2)(a).

[82] This option is contemplated by Kerber (n 81), sec 4, based on the example of smart vehicles.

[83] According to Data Act proposal, art 9.

party, thereby disincentivising third parties to engage. The reading of both Article 5(3)[84] and (5)[85] however suggests that the European Commission may have envisaged this option, while attempting to regulate the possible detrimental consequences on the third party. The opposite situation – where the data holder would not sort data out and would share all data generated by the use of the product or related service to the chosen third party – seems much less likely. This being, the Data Act proposal is actually not clear on which data the chosen third party is entitled to. In any case, it is likely to require lengthy negotiations between the data holder and chosen third party.[86]

## 2.3 Main conclusions and recommendations

The ambition of the European Commission to protect users against harmful use of data by data holders (defensive facet of data control) in laudable. However, there is room for improvement, by extending the effect of the limitations downstream the data transactions initiated by data holders. The notion of 'use' should be clarified, in particular in contrast to 'processing'. While the first sentence of Article 4(6) raises many questions, the legislator should clarify the rationale, or else a sound alternative rule should be substituted, such as a simple deletion,[87] the right for the user to request a contractual agreement on the use of data[88] and/or a list of legal bases for the processing of data by the data holder inspired by Article 6 of the GDPR.

Concerning the positive facet of data control, it is only logical that the data portability right is not subject to exhaustion, which should be clarified expressly. Besides, it may be advisable that the Data Act further regulates how to align data 'demand' and 'offer' in a certain data portability instance. Two suggestions can be made at this point. First, transparency obligations should not only be targeted at users but also at chosen third parties, possibly in the form of a right for the chosen third party to request a number of relevant further information to the data holder. Second, we posit the hypothesis that the alignment of data 'offer' and 'demand' in a given instance could constitute an activity for data intermediaries to facilitate the implementation of the data portability mechanism, as flexible and neutral market facilitators (on the role that data intermediaries could play, see section 17.5 of this White Paper).

# 3 The broadening of the right to data portability for IoT products: Who does the Act actually empower? – Daniela Spajic[89] and Teodora Lalova-Spinks[90]

[84] Article 5(3) reads as follows: 'The user or third party shall not be required to provide any information beyond what is necessary to verify the quality as user or as third party pursuant to paragraph 1. The data holder shall not keep any information on the third party's access to the data requested beyond what is necessary for the sound execution of the third party's access request and for the security and the maintenance of the data infrastructure.'

[85] Article 5(5) reads as follows: 'The data holder shall not use any non-personal data generated by the use of the product or related service to derive insights about the economic situation, assets and production methods of or use by the third party that could undermine the commercial position of the third party on the markets in which the third party is active, unless the third party has consented to such use and has the technical possibility to withdraw that consent at any time.'

[86] This was the warning raised by Kerber (n 81), sec 4.

[87] Preferred option according to Drexl and others (n 74) para 54.

[88] This is the 'second best' suggestion by Drexl and others (n 74) para 53.

[89] Doctoral researcher at Centre for IT & IP Law (CiTiP), KU Leuven, Belgium.

[90] Clinical Pharmacology and Pharmacotherapy, Department of Pharmaceutical and Pharmacological Sciences, KU Leuven, Belgium. Doctoral researcher at Centre for IT & IP Law (CiTiP), KU Leuven, Belgium. The authors have contributed equally to this work.

In light of the European Commission goal to create a data-agile economy, the empowerment of data subjects is currently at the centre of new EU policy initiatives.[91] The notion of empowerment is often equated with the strengthening of control over one's own personal data. It typically pertains to individuals and their empowerment through tools such as consent and the data subjects' rights. Especially the right to data portability enshrined in Article 20 GDPR is increasingly promoted as an essential tool, perhaps even as the main tool, to 'further strengthen' control of data subjects.[92] Yet, the Data Act proposal[93] introduces a substantial shift in the discourse about the data portability right and individual empowerment.

## 3.1 The Data Portability Right: Version 1.0, 2.0, 3.0, …

The GDPR was the first EU regulation to introduce a right to data portability. Pursuant to Article 20 GDPR, data subjects have the right to receive personal data concerning them and to transmit those data to another controller. The scope of the right, however, is fairly limited: first, the right can only be exercised where the processing of personal data is based on consent or contract and carried out by automated means.[94] Second, it applies only to personal data that was provided by the concerned data subject. Third, the transmission from one controller to another must be technically feasible.[95]

Despite its limited field of application, data portability as a tool is considered to be a key enabler to foster data sharing and to advance the data economy.[96] Therefore, it is not a surprise that the Data Act aims to broaden its scope in order to enable the re-use of data in a larger set of contexts.

### 3.1.1 Data portability in the Data Act

Put in concrete terms, the Data Act 'enhances' the data portability right for IoT products in the following ways:

1) the proposal extends the right to data portability from natural to legal persons;

2) the legal basis for the original processing of personal data is no longer limited to consent or contract but applicable to data processing based on any legal basis;

3) the right applies to the use of personal and non-personal data, as the applicable provision refers to any 'data generated by the use of a product or a related service';[97]

[91] Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A European Strategy for Data, COM(2020) 66 final (Communication 'A European Strategy for Data').
[92] Ibid 10, 20.
[93] 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 (Data Act proposal).
[94] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L 119/1 (GDPR), art 20(1)(a-b).
[95] GDPR, art 20(2).
[96] Communication 'A European Strategy for Data', 20-21.
[97] Data Act proposal, art 4(1).

4) the Data Act proposal explicitly specifies that the right applies to both 'actively provided' data, as well as 'passively observed' data (Recital 31 DA) [98] and finally;

5) the proposal mandates and ensures the technical feasibility of third-party access for all types of data (personal and non-personal),[99] thus going beyond the technical obligations prescribed in Article 20 GDPR (only for personal data).

Although the Data Act is the proposal that imposes the most significant changes to the right to data portability, the recently published proposal for a European Health Data Space Regulation (EHDS)[100] and the Data Governance Act[101] deserve mention as all three frameworks complement each other.

### 3.1.2 Data portability in the European Health Data Space

It is important to note that the recently published proposal for an EHDS broadens the scope of the right to data portability for the health sector yet again, thereby creating a sort of a third version of the concept. The proposal aims to ensure that 'data subjects can transmit their electronic health data, including inferred data, irrespective of the legal basis for the processing of the electronic health data'.[102] Unlike the Data Act proposal, EHDS' provisions afford the right to portability only to natural persons. But, same as the Data Act proposal, the right applies to both personal and non-personal data, as the EHDS introduces the notion of 'electronic health data' encompassing both personal and non-personal (electronic health) data.[103] Additionally, whilst the Data Act excludes 'inferred' or 'derived' data from its scope of application,[104] the EHDS includes 'inferred' and 'derived' data (including data obtained during a medical examination) as well as 'observed' and recorded data by automatic means into the scope of the right to data portability.[105] The Article 29 Working Party provided some clarification on these notions.[106] However, it remains unclear how the terms 'inferred', 'derived', and 'observed' data (used in the EHDS proposal) relate to the concepts of 'actively provided' and 'passively observed' data (under the Data Act proposal), as the Data Act proposal does not define the latter (on the lack of clarity of these notions, see also sec. 15.3 of this White Paper).

### 3.1.3 What about the Data Governance Act?

With a view to the DGA, data portability is expected to be one of the key enablers of altruistic data sharing and the re-use of personal data for scientific research purposes.[107] Notably, the right to data portability is not embedded in the DGA as such. Rather, the European data altruism consent form builds on this right since it should foster data portability 'where the data to be made available is not

[98] Ibid, rec 31.
[99] Ibid.
[100] Commission, 'Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space' COM/2022/197 final (EHDS proposal).
[101] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 [2022] OJ L 152/1 (DGA).
[102] EHDS proposal, rec 12.
[103] Ibid 2(2)(a-c).
[104] Data Act proposal, rec 14.
[105] EHDS proposal, rec 5.
[106] Article 29 Working Party, 'Guidelines on the right to data portability under Regulation 2016/679' WP242 rev.01, 10.
[107] Julie Baloup, Emre Bayamlıoğlu, Aliki Benmayor, Charlotte Ducuing, Lidia Dutkiewicz, Teodora Lalova, Yuliya Miadzvetskaya, Bert Peeters, 'White Paper on the Data Governance Act' (2021) CiTiP Working Paper, 38 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3872703> accessed 10 October 2022.

held by the individual'.[108] For the empowerment of individuals, the DGA foresees the help of data intermediaries in supporting them with regard to the enforcement of their rights related to their personal data.[109]

## 3.2 Questioning the data portability new clothes

On the surface, the new 'enhanced' versions of the right to data portability appear to serve the goal of individual empowerment by remedying the limitations enshrined in the GDPR. However, a careful critical discussion of the broadened scope(s) of the right appears highly necessary to ensure that the individuals who will be empowered with the mechanisms are indeed, the individuals. For this section, we focus on highlighting several key uncertainties created through the broadening of the scope under the Data Act proposal.

### 3.2.1 Quid individual empowerment?

While broadening the scope of the data portability right may be generally welcome, it raises issues regarding the notions of individual empowerment and data control. Both notions were in the GDPR firmly linked to the personal data protection of data subjects, whereas the Data Act suggests extending data subjects' rights to legal persons. More specifically, the Data Act proposal moves away from the legal terminology introduced by the GDPR and establishes instead the notion of 'user', which refers to a 'natural or legal person that owns, rents or leases a product or receives a service'.[110] Users are afforded a right to access and use data generated by the use of products or related services [111] that could be perceived as a broadened right to data portability which commercial businesses could exercise.[112] This can be concluded based on a combined reading of the explanatory memorandum, the Impact assessment report that accompanies the Data Act proposal, and relevant recitals in the Data Act proposal (for example, Recital 31), even if it is not explicitly named as such in the law.

The opening of the data portability right to legal persons under the Data Act needs to be carefully examined. The Data Act proposal does establish safeguards against potential misuse of the portability right by legal persons, namely by stating that

> [w]here the user is not a data subject, any personal data generated by the use of a product or related service shall only be made available by the data holder to the user where there is a valid legal basis under Article 6(1) of Regulation (EU) 2016/679 and, where relevant, the conditions of Article 9 of Regulation (EU) 2016/679 are fulfilled.[113]

However, would this be sufficient to ensure that no misuse occurs? Moreover, the reasoning of focusing on 'user' empowerment (in contrast to individual empowerment) is not made clear in the

[108] Commission, 'Proposal for a Regulation of the European Parliament and the Council on European data governance (Data Governance Act)' 8 COM(2020) 767 final, Explanatory memorandum.
[109] DGA, rec 30.
[110] Data Act proposal, art 2(5).
[111] Ibid, art 4.
[112] EDPB, EDPS, 'EDPB-EDPS Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)' 10 (2022).
[113] Data Act proposal, art 4(5).

Data Act proposal and its accompanying documents, especially as regards to the empowerment of legal persons over the use and portability of data subjects' personal data.

### 3.2.2 Data portability for personal and non-personal data

Furthermore, the broadening of the data portability right and its application irrespective of the legal ground on which the data processing is initially based, raises questions as regards to how the Data Act proposal has to be read or applied in conjunction with the GDPR. Regarding data portability, the Data Act gives users a right to share data (meaning in general terms any personal or non-personal data) with third parties irrespective of the legal ground based on which the processing of personal data takes place.[114] However, the enforcement of the data portability right by individuals under the GDPR is limited, so that only personal data can be ported when the data processing activity is based on consent and contract. Hence, there is a clear tension between Article 20 GDPR and Article 5 Data Act proposal regarding the scope of application, creating legal uncertainty on the porting or sharing of personal data requested by data subjects. This tension leads to the question as regards to the application of the Data Act proposal vis-à-vis the GDPR: should the Data Act proposal be applied as 'lex specialis'? The Data Act proposal appears to speak against such a view, as Article 1(3) Data Act proposal refers to Article 20 GDPR and states that the Data Act proposal 'shall complement the right of data portability under Article 20' GDPR where the personal data of users who are data subjects are concerned.[115] Consequently, if Article 20 GDPR is the relevant provision to be relied upon for the porting of personal data, then the provisions of the GDPR will collide with the Data Act proposal due to the limited scope of the data portability right under the GDPR.

## 3.3 Conclusion

With the entry into force of the Data Act proposal and the EHDS, we will have three different versions of the data portability right at our disposal. However, the rights differ not only in terms of scope but also by the terminology employed to describe them and enshrine them under the law. It remains to be explored how the three rights would apply in practice and, even more so, how the technical interoperability thereof will be guaranteed.

# 4 Chapter III – Making data available under FRAND terms – Charlotte Ducuing[116] and Luca Schirru[117]

## 4.1 FRAND Terms in the Data Act Proposal

'FRAND terms' stands for Fair, Reasonable and Non-Discriminatory terms. The content, and even the words, of what constitutes 'fair', 'reasonable' and 'non-discriminatory' may vary according to the regulation and/or sector under analysis.[118] Under the Data Act proposal,[119] specifically its Chapter III,

[114] Ibid, art 5.
[115] See also Data Act proposal, art 5(7), and EDPB-EDPS (n 113) 9.
[116] Doctoral researcher at Centre for IT & IP Law (CiTiP), KU Leuven, Belgium.
[117] Postdoctoral researcher at Centre for IT & IP Law (CiTiP), KU Leuven, Belgium.
[118] On this, see in particular the analysis in Mathew Heim and Igor Nikolic, 'A FRAND Regime for Dominant Digital Platforms' (2019) 10 (1) JIPITEC <https://www.jipitec.eu/issues/jipitec-10-1-2019/4883> accessed 18 October 2022.
[119] 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 (Data Act proposal), arts 8 and 9.

the making available of data, the compensation for such and dispute settlements relating to it, should all be governed by FRAND terms.

FRAND terms – or 'quasi-FRAND', that is, without the 'reasonability' requirement, which is sometimes substituted by more sophisticated (price) regulation - constitute a well-known tool. FRAND terms stem from competition law[120] and have been laid down in competition law-inspired regulation such as mandatory licences (for example, for essential standards) in Intellectual Property (IP), and in the long-lasting regulation of liberalised network industries.[121] Despite not using the exact words for the reasonability, fairness and non-discrimination, FRAND-based structures can be found, for example, in the Vehicle Emissions Regulation, the Horizon 2020 programme, among different regulations applicable to multiple sectors.[122] They have increasingly made their way to information-sharing obligations. For example, quasi-FRAND terms are applicable to the sharing of existing data in the case of registered substances under the Regulation for the Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH),[123] public sector bodies shall apply quasi-FRAND conditions when making data available under Chapter II of the DGA.[124] The EC proposal for a Digital Markets Act also refers to FRAND terms concerning the regulation of online gatekeepers, and in particular the provision to third-party providers of online search engines with access to ranking, query, click and view data in relation to search generated by end users of the gatekeeper.[125]

FRAND terms are not homogeneous. They are sometimes accompanied by more specific rules (often concerning price setting). A crucial question relates also to who determines the application of FRAND terms – whether a general statutory obligation or an ad hoc decision by an enforcement authority – and who substantiates FRAND terms, when (that is, whether ex ante or ex post) and based on which criteria and objectives. Such factors obviously have a determining impact. In particular, while FRAND terms are often expected to constitute a middle ground between (deemed intrusive) rule-based regulation and the freedom to conduct a business, they may eventually lead to - more or less 'soft law'

[120] On the origins of FRAND terms, see Yann Ménière, 'Fair, Reasonable and Non-Discriminatory (FRAND) Licensing Terms: Research Analysis of a Controversial Concept' (JRC Science and Policy Report, European Commission, 2015) sec. 3.

[121] The latter are surprisingly often overlooked in review on FRAND terms. However, they constitute a major tool in the regulatory toolbox and, therefore, an interesting source of inspiration. See for example under the European Electronic Communications Code, among others art 57(4) ('Deployment and operation of small-area wireless access points'). Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (recast) [2018] OJ L 321/36 (European Electronic Communications Code). National Regulatory Authorities may also impose FRAND terms for the mandatory access to some facilities by operators (art 61(2)(d). The regulation of the conditions of access to the railway infrastructure and to the related services is also strongly inspired by FRAND terms, although the price is regulated more in details by statutory regulation, see in particular Directive 2012/34/EU of the European Parliament and of the Council of 21 November 2012 establishing a single European railway area (recast) [2012] OJ L 343/32, arts 13 and 31. See also the cross-sectoral Broadband Cost Reduction Directive, among others, art 3(5). Directive 2014/61/EU of the European Parliament and of the Council of 15 May 2014 on measures to reduce the cost of deploying high-speed electronic communications networks [2014] OJ L 155/1 (Broadband Cost Reduction Directive)

[122] See the (non-exhaustive) outline of FRAND terms applicable in EU law, Heim and Nikolic (n 119).

[123] Regulation (EC) No 1907/2006 of the European Parliament and of the Council of 18 December 2006 concerning the Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH), OJ L 396/1, art 27.

[124] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 [2022] OJ L 152/1 (DGA), art 5(2). Quasi-FRAND terms are also applicable to public sector bodies under the Open Data Directive (art 8) although, in such case, however, the Directive further regulates the price (see art 6). Data intermediaries regulated under Chapter III of the DGA shall also abide by quasi-FRAND terms, which apply however to the "procedure for access to [their] service", and not to the (including, pricing) conditions for providing such services, DGA, art 12(f).

[125] Commission, 'Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act)' COM/2020/842 final (DMA proposal), art 6(1)(j).

regulatory - price-setting by enforcement authorities.[126] In any case, the interpretation of FRAND terms is often complex, as analysed, for example, in the field of standard essential patents (SEP).[127]

According to arts 8, 9 and 10 of the Data Act proposal, the making available of data from a data holder to a data recipient[128] must be done under fair, reasonable and non-discriminatory terms. Here, 'making available' shall encompass the discussion and agreement on the terms under which data will be made available[129] and the compensation for making data available.[130] Furthermore, to 'settle disputes in relation to the determination of fair, reasonable and non-discriminatory terms for and the transparent manner of making data available (...)', access to dispute settlement bodies shall be granted to both parties.[131] As seen in the Impact Assessment for the Data Act proposal, the European Commission views FRAND terms pursuant to Chapter III as a fall-back for competition law. They shall constitute a middle ground between 'a patchwork of sector-specific rules', deemed inefficient, and 'over-regulation [i.e.] by setting very detailed requirements', deemed not fit for 'dynamically evolving technological requirements'.[132]

## 4.2 Are FRAND terms in the Data Act proposal adequate?

The introduction of FRAND terms applicable to all future obligations to make data available (under the conditions laid down in Article 8(1) of the Data Act proposal) builds on already existing patterns while at the same time constituting a breakthrough.

What is different with Chapter III of the Data Act, is the accumulation of the following elements. First and commonplace, in contrast to other things, data do not have a (property) legal status, they are also non-rivalrous (in other words, the consumption of one unit does not subtract from the resource pool and, therefore, does not affect its availability for further consumption by others)[133] and easily duplicable. The Data Act proposal takes the de facto control of data by the data holder as a starting point for making data available.[134] This stands for example in stark contrast with FRAND terms that apply to (tangible or intangible) goods protected by (intellectual) property rights, the use of which is (de facto or de jure) excludable and, depending on the type of FRAND at stake, (unjustifiably) reserved

[126] See the case study of the application of the Broadband Cost Reduction Directive, Charlotte Ducuing, 'The Broadband Cost Reduction Directive: A Legal Primer in Cross-Sector Regulation of Infrastructures' (2021) 22(1) Competition and Regulation in Network Industries, sec. Price setting: From "business friendly" flexibility to regulatory setting <https://doi.org/10.1177/1783591720977098> accessed 18 October 2022. The existence of conflicting objectives, expected to be solved by 'FRAND terms' and the need for legal certainty and for a certain level of harmonisation across the EU, has led some enforcement authorities to take on a proactive regulatory role in setting the price, often based on soft law mechanisms.

[127] Oscar Borgogno and Giuseppe Colangelo, 'Data Sharing and Interoperability: Fostering Innovation and Competition through APIs' (2019) Computer Law & Security Review, sec 4.1 <https://doi.org/10.1016/j.clsr.2019.03.008> accessed 18 October 2022. This is against this background that they authors anticipatively warned against FRAND terms to regulate obligations to make data available.

[128] Data Act proposal, art 2(7): '"data recipient" means 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;'

[129] Ibid, art 8.

[130] Ibid, art 10.

[131] Ibid, art 10(1).

[132] Commission, Commission Staff Working Document 'Impact Assessment Report' accompanying the document Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act) SWD (2022) 34 final, 6-7.

[133] Benjamin Coriat, 'From Natural-Resource Commons to Knowledge Commons: Common Traits and Differences' (2011) LEM Papers Series 2011/16 <https://www.lem.sssup.it/WPLem/files/2011-16.pdf> accessed 18 October 2022.

[134] See Data Act proposal, rec 5.

by the holder.[135] This obviously complicates the valuation of the compensation and diminishes the added value of comparisons with existing FRAND terms.[136]

This is even more the case that the identification of what the subject-matter of the 'compensation' under Article 9 of the Data Act proposal is, is debatable, whether data,[137] the respective activities involved in the making available of data,[138] and/or royalties for Intellectual Property Rights (IPRs) which could be at stake upon making data available.[139] This issue is particularly complex when it comes to non-SMEs enterprises, to which '[i]t is unclear whether non-SMEs are always expected to pay the market value of the underlying data or only compensation of the costs of compliance with the access obligation to make the original data holder whole.'.[140] Even though it is not possible to precise an answer for the previous question and the criteria that must be used to define a compensation for larger companies, some ideas can be drawn from the Impact Assessment for the Data Act proposal:

> Where the recipients are larger companies the parties would have the margin to negotiate a reasonable compensation. In such cases, large companies are considered capable of negotiating conditions and any compensation taking into account factors such as prevailing market conditions and return on investment.[141]

Second, obligations to make data available within the meaning of Article 8 may happen to be laid down for a range of different reasons, which may not be strictly attributable to competition law or, more generally, to addressing market failures. While undeniably stemming from competition law-inspired remedies and regulation, it is also true that FRAND terms have been imposed for a growing number of other rationales already.[142] On this matter, it is worth mentioning that adopting a competition law

---

[135] On this, see 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', International Review of Intellectual Property and Competition Law Forthcoming (2022): 8, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4119834. Most authors discuss mainly FRAND in the context of IPRs and intangibles. However, FRAND terms are also commonly imposed concerning tangibles, such as in the field of liberalised network industries or utilities. In such cases in particular, FRAND terms may notably be imposed irrespective of whether the asset or system is reserved by the holder. See, for example, in the railways, Directive 2012/34/EU of the European Parliament and of the Council of 21 November 2012 establishing a single European railway area (recast), OJ L 343/32. Ex ante and regulatory nature of the legal regime.

[136] On similar concerns, see 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) https://pure.mpg.de/rest/items/item_3388757_4/component/file_3395639/content> accessed 7 October 2022, para 102.

[137] Rec 42 states that '[…] these provisions should not be understood as paying for the data itself […]". However, when dealing with the question how the compensation shall be calculated in the case where the data recipient is not an SME, rec 46 states that '[…] in such cases, the companies are considered capable of negotiating any compensation if it is reasonable, taking into account facts such as the volume, format, nature or supply of and demand for the data as well as the costs for collecting and making the data available to the data recipient'. This seems to suggest that the compensation should also relate to data, in addition to the activity of make them available. On this, see also Charlotte Ducuing, 'An Analysis of IoT Data Regulation under the Data Act Proposal through Property Law Lenses' (2022) CiTiP Working Paper 2022, sec 5 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4225027> accessed 7 October 2022

[138] On the activities necessary to make data available in the case of Chapter II, see sec 2.

[139] Wolfgang Kerber, 'Governance of IoT Data: Why the EU Data Act will not Fulfill Its Objectives (second version)' (2022) GRUR International, 21-22 (forthcoming as third, revised version), sec 4.3. <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4080436> accessed 18 October 2022. On the lack of clarity of the compensation regulation, see Inge Graef and Martin Husovec, 'Seven Things to Improve in the Data Act' (2022), sec. 4, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4051793> accessed 18 October 2022.

[140] Graef and Husovec, n (140) 3.

[141] Commission, Commission Staff Working Document 'Impact Assessment Report' accompanying the document Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act) SWD (2022) 34 final, 154

[142] Heim and Nikolic, (n 119) para 2.

rationale/tool or a different one when it comes to FRAND-based terms should not be an exclusive option, as mentioned by Habich:

> (...) the application of the Data Act, the Digital Markets Act and competition law is not mutually exclusive, as the DA and DMA regulate overlapping constellations of mandatory data access. Namely, Art. 8(1) DA extents the FRAND obligations of Chapter III and IV DA not only to data holders obliged to make data available under the Data Act, but to all data holders obliged to make data available under Union Law.[143]

Against this background, it could be argued, at first glance, that the imposition of FRAND terms for the making available of data under Chapter III, for reasons possibly entirely alien to competition law does not raise new issues.

This being, the Data Act proposal goes yet a step further by laying down rules – that is, FRAND terms – even prior to the identification of any rationale. In other words, FRAND terms are seemingly viewed as a solution to all problems that could lead to future obligations to make data available to businesses. The scope is both very broad and unclear ('where a data holder is obliged to make data available to a data recipient (…)'), as further discussed in Sec. 6), which is again reinforced by the broad and unclear definition of 'data'.[144] While the European Commission demonstrably drafted Chapter III with competition concerns in mind, it cannot be excluded that they end up applying to legislations for which they simply don't make any sense (on the unclear notion of 'obligation to make data available', see sec. 6.2 in this White Paper).[145]

For instance, pursuant to the Commission Delegated Decision 2017/1474, the European Technical Specification Interoperability concerning Telematics Applications for Passenger Services (TAP TSI),[146] dealing with the exchange of electronic messages for the operation of passenger trains, shall be revised to include data exchange with safety related applications.[147] In the Commission Staff Working Document on Common European Data Spaces, the European Commission confirmed its willingness to revise the TAP TSI.[148] Should it occur, such revision could easily fall in the scope of Chapter III, with the ensuing application of FRAND terms. However, the TAP TSI is limited in scope to the technical facilitation of the exchange of messages for the operation of trains. It is hard to see how FRAND terms could find a useful application here, or else this could change the general balance of the legal framework.

---

[143] 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) International Review of Intellectual Property and Competition Law, 8 (forthcoming) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4119834> accessed 18 October 2022.

[144] Julie Baloup and others, 'White Paper on the Data Governance Act' (2021) CiTiP Working Paper 2021, sec 2.1. <https://papers.ssrn.com/abstract=3872703> accessed 18 October 2022.

[145] Similarly, see Drexl and others (n 137) paras 103–105. Besides, the Max Planck Institute Statement suggests that the jurisdiction of DSBs shall be extended to the whole dispute at stake between the data holder and data recipient, which may indeed extend beyond the sole 'data' aspect, Drexl and others, para 108. However, this recommendation is rendered unfeasible by the uncertainty surrounding the future obligations to make data available, as well as, relatedly, the context in which disputes could therefore arise. Extending the jurisdiction of dispute-resolution bodies to the whole dispute at stake would amount to simply giving them a blank cheque.

[146] Commission Regulation (EU) No 1305/2014 of 11 December 2014 on the technical specification for interoperability relating to the telematics applications for freight subsystem of the rail system in the European Union and repealing the Regulation (EC) No 62/2006 [2014] OJ L 356/438 (TAF TSI).

[147] Commission Delegated Decision (EU) 2017/1474 of 8 June 2017 supplementing Directive (EU) 2016/797 of the European Parliament and of the Council with regard to specific objectives for the drafting, adoption and review of technical specifications for interoperability [2017] OJ L 210/5, art 13(4).

[148] Commission Staff Working Document on Common European Data Spaces, SWD(2022) 45 final, 20.

## 4.3 Conclusion

The specific characteristics of data and the broad and cross-sectional approach brought by the Data Act present some challenges to the adoption of FRAND terms including, but not limited to, the definition of what should be a 'reasonable compensation' for making data available, which should be the criteria to reach this reasonableness and the need for the 'data holder to provide access without undue delay under Article 4(1).[149] The imposition of FRAND terms for virtually all future obligations to make data available, irrespective of the objective pursued, does not have a clear and duly motivated rationale and may simply prove inappropriate in some cases. Against this background, it has to be concluded that FRAND terms as per Chapter III of the Data Act proposal are very unlikely to deliver on the expectations to provide a baseline law for data spaces, viewed by the Commission as a middle ground between (a) rule-based legislation and the freedom to conduct a business on the one hand and (b) lex generalis and (sector or data space)-specific rules on the other.

More generally, there is a visible trend towards a generalisation of obligations to 'be kind' - in other words, at least transparent, fair and non-discriminatory - in EU legislations, especially in the digital environment.[150] FRAND terms, and more generally the obligation to be 'fair', are visibly viewed as a means to future-proof legislation[151] in the face of the fast pace of innovation. But to what extent they can be duplicated to all sorts of (regulatory) contexts should be further analysed, while the example of the Data Act shows that this is not without raising issues.

# 5 Chapter III, Article 11 of the Data Act – The regulation of unauthorised access to data – Leander Samuel Stähler[152]

## 5.1 Introduction

Article 11 of the proposed Data Act regulates 'technical protection measures and provisions on unauthorised use or disclosure of data'.[153] As this section argues, the key notion of 'unauthorised access' will likely contribute to interpretational tensions. Additionally, drawing upon the EU copyright acquis, it is argued that potential intersections with existing law may be particularly problematic in delineating this notion.

### 5.1.1 Article 11

Facially, Article 11(1) states that the 'data holder may apply appropriate technical protection measures, including smart contracts, to prevent unauthorised access to the data and to ensure compliance with Articles 5, 6, 9 and 10, as well as with the agreed contractual terms for making data available'. Article 11(1) clarifies that the application of TPMs should not affect the user's right to 'effectively provide data to third parties (…) or any right of a third party' pursuant to Articles 5 and (8(1)).

[149] Drexl and others (n 137) 33-34.

[150] This is obviously the case in the Data Act but also in the DMA, art 6, incumbent on online gatekeepers, and under the DGA, Chapter III, incumbent on data intermediaries.

[151] On future-proving legislation, see Sofia Ranchordas and Mattis Schip van't, 'Chapter 16. Future-Proofing Legislation for the Digital Age', in *Time, Law and Change - An Interdisciplinary Study*, Sofia Ranchordás and Yaniv Roznai (Hart Publishing, 2020), 347–65.

[152] Doctoral researcher at Centre for IT & IP Law (CiTiP), KU Leuven, Belgium.

[153] 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 (Data Act proposal), art 11.

Further, Article 11(2) provides that upon performing acts, such as the provision of false information or the abuse of evident gaps in infrastructure to obtain data, a data recipient 'shall without undue delay, unless the data holder or the user instruct otherwise': (a) destroy the data acquired, and; (b) end the use of goods, 'derivative data' or services produced 'on the basis of knowledge obtained through such data'.[154] Article 11(3) excludes the obligation in paragraph (2)(b), where there is no significant harm to the data holder or where it would be disproportionate in light of the data holder's interests.

### 5.1.2 The Structure of Article 11

Article 11 regulates a particular structure between data holders, users and data recipients, all of which have specific definitions under Article 2 (see also Figure 1):

- Article 11(1) allows only the data holder to apply TPMs, limited by the right of the user to share data with third parties – it provides that data holders 'may' apply TPMs for the above purpose of preventing unauthorised access;

- Article 11(2) creates obligations for data recipients (who act for a business purpose) and allows both the data holder and the user to instruct a data recipient to not delete data or end the use of goods and services;

- Article 11(3) only considers the harm to and interests of the data holder.

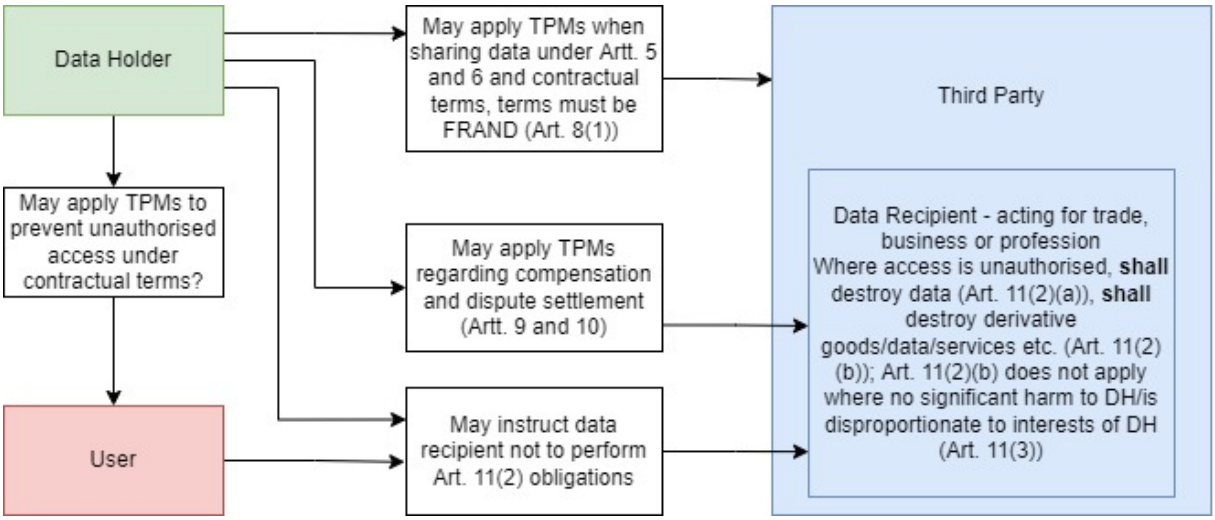


**Figure 1: The Structure of Article 11**

## 5.2 Unauthorised Access to Data

### 5.2.1 Unauthorised Access under Article 11

[154] Full text: "A data recipient that has, for the purposes of obtaining data, provided inaccurate or false information to the data holder, deployed deceptive or coercive means or abused evident gaps in the technical infrastructure of the data holder designed to protect the data, has used the data made available for unauthorised purposes or has disclosed those data to another party without the data holder's authorisation, shall without undue delay, unless the data holder or the user instruct otherwise: (a)destroy the data made available by the data holder and any copies thereof; (b) end the production, offering, placing on the market or use of goods, derivative data or services produced on the basis of knowledge obtained through such data, or the importation, export or storage of infringing goods for those purposes, and destroy any infringing goods." Data Act Proposal, art 11(2).

Within the context of the Data Act proposal, Article 11 introduces the undefined notion of 'unauthorised access' to data. As shown in Figure 2, this notion serves as a cumulative pre-condition subject to which the data holder may apply TPMs,[155] and should therefore be a clear notion for the proper functioning of the provision. To wit, 'unauthorised access' suggests that access to relevant data can be authorised. The below holistically interprets 'unauthorised access' as a notion of the Data Act with a focus on Article 11, arguing that the notion suffers from deficiencies in clarity as indicated by plausible data exchange situations.

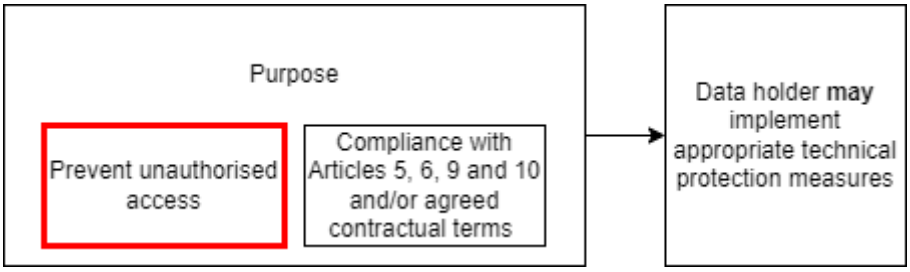


**Figure 2: Unauthorised Access**

Firstly, the notion of unauthorised access is particularly unclear for a data exchange between a data holder and a user. The inclusion of 'agreed contractual terms' in Article 11(1) can reasonably be understood to encompass contractual terms between data holder and user.[156] This could entail, depending on the contract in question, that authorisations can be provided by either the data holder or the user. From the perspective of the data holder, a data holder may therefore interpret that they must provide access to the user as outlined in Chapter II. Access to data beyond the Chapter II requirements may therefore fall under 'contractual terms' in the sense of Article 11(1),[157] and the data holder may plausibly apply TPMs to ensure this. As Kerber argues,[158] data holders thus retain a high level of de facto control of data.

From the user perspective, users may also interpret 'unauthorised access' in their interest. As suggested in the recitals,[159] a user can limit the access of a data holder to the data held and plausibly require the data holder to apply TPMs to ensure this. Both perspectives indicate that authorisation of access may differ on a case-by-case basis, with potential implications for how the data holder may apply TPMs.

[155] For the sake of graphical clarity, Figure 2 shows unauthorized access separate from the category of 'compliance with Articles 5, 6, 9 and 10 and/or agreed contractual terms' – this is not to prejudice the joint interpretation of these pre-conditions.

[156] Art 11(1) is a 'may' provision and does not indicate whether or not TPMs are prohibited from being applied for a purpose different from those explicitly mentioned by the provision.

[157] Notably, derivative data is not considered data generated by the use of a product or related service, and thus falls outside the scope of data to be made available to the user (Data Act proposal, rec 17). A similar but distinct situation is presented by data that is considered by the data holder to comprise trade secrets (Data Act proposal, art 4(3)).

[158] Wolfgang Kerber, 'Governance of IoT Data: Why the EU Data Act will not Fulfill Its Objectives (second version) (2022) GRUR International, 9 <https://www.ssrn.com/abstract=4080436> accessed 18 May 2022, arguing that Recital 21 limits 'access' to 'the product or on a computing instance of the manufacturer'; 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) UZH Working Paper, 4 <https://papers.ssrn.com/abstract_id=4119834> accessed 15 June 2022.

[159] 'This Regulation should not prevent contractual conditions, whose effect is to exclude or limit the use of the data, or certain categories thereof, by the data holder'. Data Act proposal, rec 24.

Secondly, the notion of unauthorised access is unclear within a data exchange between a data holder and a data recipient. Namely, Article 11(2) bifurcates the power to instruct a data recipient where the data recipient has breached TPMs (for example, by abusing evident gaps in the technical infrastructure). By allocating this authorisation *qua* instruction to both the data holder and the user, both enjoy discretion over access for individual data recipients,[160] including which TPMs apply to which data recipient. Therefore, each data holder or user may plausibly understand, based on their interests, that they are empowered to provide authorisations vis-à-vis data recipients.

Finally, there exists a lack of clarity on the notion of unauthorised access within a broader context outside the data holder-user-third party triangle (see Figure 1) under novel data governance arrangements. Namely, under the Data Governance Act, the EU legislature has adopted rules to facilitate trustworthy data sharing[161] while using a different definition of 'data holder' than that used in the proposed Data Act to delimit the party that can 'grant access' to data.[162] In the case of data regulated by the Data Act, the above shows that it may be difficult to establish which exact party fulfils this role.

Considering this, diverging interpretations of the Data Act contribute to rivalling notions of unauthorised access. A clarification of this provision should explain who can issue authorisations under which circumstances and potentially explain why the data holder has been tasked with applying TPMs, whilst both the data holder and users have interests in the data at stake. In this vein, Kerber argues that a clearer scope for Article 11 could 'reduce transaction costs and mitigate disputes significantly'.[163] This reiterates previous questions regarding 'lawful access' under the Data Governance Act.[164]

### 5.2.2 Unauthorised Access and Copyright

Further questions about interpreting 'unauthorised access' are raised by areas of law that are certain to intersect with the rules laid down by the Data Act. One such area of law is the EU copyright acquis (the EU body of law regulating copyright and related rights).

The definition of data under the Data Act covers 'any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audio-visual recording',[165] including data recorded intentionally by the user, but excluding data derived from

[160] However, art 2(7) excludes users from the scope of 'data recipient', thereby giving users the right to provide qualifying third party data recipients the power to circumvent TPMs, without being able to provide this power to themselves. Data Act proposal, art 2(7).

[161] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 [2022] OJ L 152/1 (DGA), rec 3; The DGA regulates so-called data intermediation services and data altruism organisations.

[162] That is, a data holder under the DGA is 'a legal person, including public sector bodies and international organisations, or a natural person who is not a data subject with respect to the specific data in question, which, in accordance with applicable Union or national law, has the right to grant access to or to share certain personal data or non-personal data'. DGA, art 2(8).

[163] Kerber (n 159) 15.

[164] See regarding the notion of 'data user' under the Data Governance Act, which rests upon the unclear condition of "lawful access": Julie Baloup, Emre Bayamlıoğlu, Aliki Benmayor, Charlotte Ducuing, Lidia Dutkiewicz, Teodora Lalova, Yuliya Miadzvetskaya, Bert Peeters, 'White Paper on the Data Governance Act' (2021) CiTiP Working Paper, 13 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3872703> accessed 10 October 2022; this condition has been retained in the final version of the DGA. DGA, art 2(9).

[165] Full definition: 'any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audio-visual recording'. Data Act Proposal, art 2(1).

a software process.[166] This means that there could be significant intersections between 'data' and protected subject matter under the EU copyright acquis,[167] where an author or rightsholder can be attributed to the protected subject matter.[168]

This intersection has plausible implications for the notion of 'unauthorised access' under the Data Act as the copyright acquis outlines rules on authorisations vis-à-vis protected subject matter. Namely, the copyright acquis provides a framework for statutory and voluntary authorisations for the performance of certain acts regarding protected subject matter (via exceptions and limitations and via contracts and licences, respectively). This framework will continue to apply to protected subject matter, regardless of the notion of unauthorised access under the Data Act. This is the case as the Data Act explicitly does not affect existing rules on intellectual property (except for the sui generis database right).[169]

For instance, an IoT product covered by the Data Act could record, transmit or provide access to the digital representation of subject matter covered by the EU copyright acquis, potentially interfering with the exclusive right of reproduction, the right of communication to the public and/or the right of distribution.[170] In such cases, it is not guaranteed that either the data holder, user or data recipient is the rightsholder of the protected subject matter. This means, for instance, that providing the data holder and user with discretion vis-à-vis unauthorised access under Article 11(2) could potentially infringe the rights of the relevant rightsholder under the copyright acquis in the absence of an applicable authorisation.

It is beyond the scope of this contribution to fully analyse this likely intersection of legal regimes,[171] yet 'data' that falls under the protection of the EU copyright acquis will need to consider existing rules on copyright authorisations. This particular intersection between the Data Act and copyright demonstrates the complexity of introducing the notion of “unauthorised access” and interpreting it in light of existing law.

## 5.3 Concluding Remarks

In regulating unauthorised access as a pre-condition for technical protection measures, we can identify tensions arising from different data exchange situations and from the intersecting legal regime of copyright. In moving forward with the proposal, legislative stakeholders need to reflect on the role of this notion, not only as it underscores the ability to apply TPMs, but also how it functions in particular data exchange situations, within the overarching structure of desired data governance mechanisms and within the broader context of intersecting areas of law. Combatting interpretational tensions may

[166] Data Act proposal, rec 17.

[167] For copyright, the work must be ‘original in the sense that it is the author’s own intellectual creation’. Case C-5/08 *Infopaq International A/S v Danske Dagblades Forening* [2009] ECR I-06569, 465, para 37.

[168] ’In copyright law, no work exists without an author’, see P Bernt Hugenholtz and João Pedro Quintais, ‘Copyright and Artificial Creation: Does EU Copyright Law Protect AI-Assisted Output?’ (2021) 52 IIC - International Review of Intellectual Property and Competition Law 1190, 1207ff.

[169] Data Act proposal, 5.

[170] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society [2001] OJ L 167/10 (InfoSoc Directive), arts 2-4.

[171] For the related issue of overlaps in intellectual property law, see Estelle Derclaye, ‘Overlapping Rights’, in Rochelle Dreyfuss and Justine Pila (eds), *The Oxford Handbook of Intellectual Property Law* (Oxford University Press 2017); regarding the particular overlap of copyright and trade secrets: Ulla-Maija Mylly, ‘Preserving the Public Domain: Limits on Overlapping Copyright and Trade Secret Protection of Software’ (2021) 52 IIC - International Review of Intellectual Property and Competition Law 1314.

therefore serve the Data Act's objective of facilitating access for users while protecting incentives to invest for data holders.[172]

# 6 Chapter III and IV of the Data Act – B2B data sharing and access - Emre Bayamlıoğlu[173]

Chapters III and IV of the Data Act proposal introduce interventions to the current legal landscape of B2B data sharing and access, in addition to Chapter II discussed, for example, in section 2. While Chapter IV prescribes a fairness test to be applied to voluntary contracts, Chapter III lays out general rules to comply with in case of a statutory obligation to make data available. This contribution provides a brief analysis on how these two Chapters affect B2B data sharing and access and underlines certain points that may give rise to misalignments or inconsistencies.

## 6.1. Basic architecture of B2B data sharing and access in the Data Act

Chapters III and IV of the Data Act proposal introduce interventions to the current legal landscape of B2B data sharing and access. The concerns relating to abuse of contractual imbalance and refusal to grant access in the B2B context have been the driving force behind the Chapters III and IV, which provide general rules for data access rights that the future legislation will grant and a fairness test for voluntary agreements of data sharing for the benefit of SMEs, respectively.

Chapter III provides general rules to comply with in case of an obligation to make data available. Data holders who are obliged to make data available to a data recipient (as in Chapter II or other Union law or Member State legislation) shall be subject to rules as laid out by the Chapter. Chapter IV prescribes a fairness test to be applied to voluntary contracts aiming for an effective system of protection for SMEs against unfair contractual terms in data sharing that will contribute to micro, small or medium-sized enterprises' ability to conduct a business.

These two chapters together provide a general legal framework of both mandatory (as could be prescribed law) and voluntary data access and sharing in the B2B context.

### 6.1.1. Chapter III - General rules applicable to obligations to make data available

Chapter III titled, Obligations for data holders legally obliged to make data available, provides general access rules where a data holder is obliged by law to make data available to a data recipient. Chapter III does not directly mandate data access or sharing but lays out a framework relating to the obligations to make data available. It concerns all the rules under Union law or national legislation implementing Union law, which oblige data holders to make data available. The Chapter does not apply to data access rights under the GDPR.

According to Article 8(1), a data holder who is obliged to make data available to a data recipient under Article 5 (IoT data portability) or other Union law or national legislation implementing Union law shall perform this obligation under fair, reasonable and non-discriminatory terms and in a transparent

[172] "Facilitate access to and the use of data by consumers and businesses, while preserving incentives to invest in ways of generating value through data". Data Act proposal, 3.

[173] Researcher at Centre for IT & IP Law (CiTiP), KU Leuven, Belgium.

manner. The FRAND licensing system has primarily been developed for standard essential patents.[174] It allows for taking account of the specificities of the individual case. The proposal adopts the FRAND system at the interface of statutory and contract law.[175] The aim is to ensure consistency of data sharing practices in the internal market and across sectors, as discussed in sec. 4 of this White Paper.

Chapter III applies only to legally mandated data access or sharing requirements (obligation to make data available), meaning that voluntary data sharing remains unaffected by the rules laid out by the Chapter. Article 8(1) does not specify any rights or obligations other than Article 5 of Chapter II and generally refers to data holders' obligations to make data available to a recipient (See also Article 12(1)). By virtue of Article 12(3), Chapter III only covers obligations to make data available that enter into force after the effective date of the proposed Data Act.[176] Article 8(1) further provides that the data holder should perform its obligation to make data available to a recipient (under Article 5, other Union law, or national legislation implementing Union law) in accordance with the provisions of this Chapter and Chapter IV. This means that the below-explained Article 13 (Chapter III) shall be fully complied with.

Although dealing with mandatory access to data, the Chapter prioritises the agreements between the data holder and the recipient, albeit with restrictions. Article 8(2) limits the contractual terms between the data holder and the data recipient concerning the access to and use of the data or the liability and remedies for the breach or the termination of data related obligations. Where such terms fail the fairness test provided in Article 13, they will not be binding. The same applies to contractual terms that exclude the application of, derogates from or varies the effect of the user's rights to access to IoT device/service data under Chapter II.

Under Article 8(3) data holders are prohibited from discriminating between the recipients, such as affiliated enterprises, when making data available. The onus of proof lies with the data holder where a data recipient contends that the conditions under which data has been made available are discriminatory. It will be on the data holder to demonstrate that the use of different contractual terms for making data available was not discriminatory or justified by objective reasons. To a certain extent, this prohibition parallels non-discrimination requirements under the EU competition regime (for example, Article 102 of the Treaty on the Functioning of the European Union (TFEU)). Yet, the reversed burden of proof provided by Article 8(3) of the Data Act gives rise to a stricter obligation. According to Article 8(4), data holders are also prohibited from making data available to a data recipient on an exclusive basis unless requested by the user under Chapter II.

In order to incentivise the continued investment in generating valuable data, including investments in relevant technical tools, Article 9 provides for a compensation to be paid to the data holder when fulfilling the obligation to make data available. When the recipient is a SME, the compensation for making data available should not exceed the direct cost of making the data available. In cases where

[174] FRAND terms were also used in liberalised network industries (for example, telecommunications and energy) with respect to the access to tangible assets aiming to open up markets to competition.

[175] For more on the origins, suitability and complications of the FRAND system, see 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 No. 22-05, paras 94-117 <https://pure.mpg.de/rest/items/item_3388757_4/component/file_3395639/content> accessed 7 October 2022.

[176] With respect to prior EU legislation, the Chapter III may still be used as a template for future amendments to existing rules. See rec 87 of the Data Act proposal.

the data holder is a SME and the data recipient is a large company, parties are deemed capable of negotiating a reasonable amount of compensation.

Article 10 provides for a dispute settlement mechanism where certified bodies will assist parties that disagree on the compensation or on the data use. Dispute settlement under Article 10 does not directly apply to the cases of unfair contract terms unless triggered indirectly via Chapter III.[177]

Regarding technical protection measures which implement access rights and contractual terms relating to making data available, Article 11 requires that such technical measures should not be used in a way that hinders the user's right under Article 5 or any right of a third party under Union law or national legislation implementing Union law as referred to in Article 8(1).

Article 12 explicitly states that the Chapter only applies to Article 5 or other obligations under Union law or national legislation implementing Union law, to make data available to a data recipient[178] and further provides that '[a]ny contractual term in a data sharing agreement which, to the detriment of one party, or, where applicable, to the detriment of the user, excludes the application of this Chapter, derogates from it, or varies its effect, shall not be binding on that party'. [179]

### 6.1.2. Chapter IV - Unfair terms in voluntary contracts

When negotiating access to data, a party in a stronger bargaining position could leverage such a position to the detriment of the weaker party. Chapter IV of the proposal lays out a fairness test to prevent the exploitation of contractual imbalances to the detriment of SMEs. The Chapter is guided by the fact that in the B2B context, unequal distribution of bargaining power between the parties adversely affects data sharing and access, especially where the weaker party depends on access to data controlled by the other party.

Under Article 13, unfair contractual terms (concerning the access and use of data and the ensuing liability) which are unilaterally imposed on SMEs shall not be binding.[180] The scope of the Chapter is limited to SMEs, and the specific reference to enterprises as the imposing party results in a scenario where those non-profit associations and public bodies are not subject to obligations laid out by Chapter IV. Article 13 does not apply to the parts of the contract which are not related to making data available, in particular, the contractual terms defining the main subject matter of the contract or determining the price to be paid.

Pursuant to Article 13(1), the Chapter has a broad scope covering any 'contractual term, concerning the access to and use of data or the liability and remedies for the breach or the termination of data related obligations.' This includes contractual terms relating to the fulfilment of obligations for making data available, and it is further confirmed by Article 8(2) of Chapter III which states that Article 13 is

[177] Zohar Efroni, Prisca V Hagen, Lisa Völzmann, Robert Peter, Mariam Sattorov, 'Position Paper regarding Data Act (Proposal of the European Commission, 23.02.22)' (2022) Weizenbaum Policy Paper, 2, 20 <https://doi.org/10.34669/WI.WPP/2>.

[178] Data Act proposal, para 1.

[179] Ibid, para 2.

[180] Although the proposal aligns with the Directive on unfair terms in consumer contracts , it differs from it in terminology by using the term 'unilaterally imposed' instead of 'not individually negotiated' in art 3 of the latter. Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts [1993] OJ L 95/29 (Directive on unfair terms in consumer contracts).

also applicable to the terms of the contract that the parties conclude in the framework of mandatory data access regimes.[181]

The Article handles unfair contractual terms in three paragraphs. Under Article 13 (2), contractual terms that grossly deviate from good commercial practice in data access and use and that are contrary to good faith shall be deemed unfair. Article 13(3) declares unfair the contractual terms that: i) exclude or limit liability for intentional acts or gross negligence; ii) exclude the remedies or liabilities in case of non-performance; or iii) unilaterally authorise the imposing party to determine whether the data supplied are in conformity with the contract or to interpret any term of the contract. Article 13(4) describes a second group of contractual terms presumed to be unfair. These are terms which: i) allow the imposing party to access and use the data of the SME in a manner significantly detrimental to the legitimate interests of the SME; ii) prevent or limit the SME from using or obtaining a copy of the data contributed or generated by the SME during the period of the contract; and iii) enable the imposing party to terminate the contract with unreasonably short notice. 'If a contractual term is not included in the list of terms that are always considered unfair or that are presumed to be unfair, the general unfairness provision applies. In this regard, the terms listed as unfair terms should serve as a yardstick to interpret the general unfairness provision.'[182]

Under Article 13(5), the term provided by one contracting party without the other party's (namely the SME) influence on the content of the term, despite the attempts to negotiate, will be regarded as unilaterally imposed. Accordingly where the SME accepts the contractual term without any opposition or resistance, Article 13 will not apply. Recital 52 states that rules on contractual terms should consider the principle of contractual freedom as an essential concept in business-to-business relationships. Article 13 particularly concerns 'take-it-or-leave-it' situations where one party imposes a certain contractual term. 'A contractual term that is simply provided by one party and accepted by the micro, small or medium-sized enterprise or a term that is negotiated and subsequently agreed in an amended way between contracting parties should not be considered as unilaterally imposed.'[183]

## 6.2. Assessment and recommendations

The proposal (including the recitals and other explanatory parts) present certain ambiguities about the interpretation and application of Chapters III and IV.

To begin with, it is difficult to determine the exact scope of the data holder's obligation to make data available to a data recipient under Union law or national legislation implementing Union law (Article 8(1)). The provision seems to point to sector-specific data sharing and access rules enacted under the upcoming legislative initiatives for the establishment of European Data Spaces. Yet, there is no clarity to this effect and the term 'to make data available to a data recipient' is broad enough to cover various types of obligations which could be imposed by the future legislation on data holders. The limitation of the application of Chapter III to Union law or national legislation implementing Union law that enters into force after the date of application of the Data Act does not adequately solve the problem. In its current form, various obligations introduced by the current proposals of the EU commission could be

[181] See also art 8(1).
[182] Data Act proposal, rec 55.
[183] ibid, rec 52.

interpreted as an obligation to make data available to a data recipient.[184] (if it enters into force after the Data Act) business users of gatekeeper platforms will have access to the data they generate in their use of the platform. Similarly, the proposed DSA[185] obliges 'very large online platforms' to provide data access to 'vetted researchers (...) for the sole purpose of conducting research that contributes to the identification and understanding of systemic risks'. Therefore, a better option would be to clarify that Chapter III would apply to future data obligations or access rights only where there is an explicit reference to the Data Act.

The obscurity of the scope ('obligation to make data available') further aggravates the ambiguity that lies in the reference (in Article 8(1)) to the fairness test of Article 13 (Chapter IV). The question arises of how contractual principles of fairness in Article 13 could apply in connection with the performance of a mandatory obligation to make data available. Article 8(2), referring to an agreement (between the data holder and the data recipient), gives the impression that future obligations to make data available are envisaged as compulsory contracts. However, this is not clear since the first and second paragraphs of Article 8 do not properly align on this matter. That is, while the first paragraph speaks of a statutory obligation to make data available under other Union law or national legislation implementing Union law, the second paragraph treats this obligation like a contract where parties agree on the terms for making data available. Unless considered in the context of a compulsory contract, it is unclear how the fairness rules in Article 13 could apply to a statutory obligation to make data available. Hence, it is advisable that the Act provides more clarity about what the 'obligation to make data available' exactly refers to. Recital 40 also adds to the ambiguity as it states, '[i]n order to ensure that the conditions for mandatory data access are fair for both parties, the general rules on data access rights should refer to the rule on avoiding unfair contract terms.' There is still some obscurity about whether the recital is addressed to parties of the contract or[186] to Chapter IV in Chapter III. On top of those, there is the question of the application of Article 13 to obligations to make data available would also be limited to the cases where the data recipient is an SME.[187]

Considering the reference made by Article 8(2), It is also unclear what is meant by the 'conditions' of Article 13 and how it differs from Article 8(1), which requires the fulfilment of obligations for making data available in accordance with the Chapter IV (Article 13). There is also a need to define whether Article 13 should be considered to protect both data recipients and data holders.[188] Overall, the relationship between the FRAND principles in article 8 and the fairness test in Article 13 needs to be better explained.

---

[184] Under the DMA proposal art 6(g), a gatekeeper shall provide advertisers and publishers, upon their request and free of charge, with access to the performance measuring tools of the gatekeeper and the information necessary for advertisers and publishers to carry out their own independent verification of the ad inventory and under art 6(h) provide effective portability of data generated through the activity of a business user or end user and shall, in particular, provide tools for end users to facilitate the exercise of data portability. Also see art 6(i) and (j). Commission, 'Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act)' COM/2020/842 final (DMA proposal). Commission, 'Proposal for a Regulation of the European Parliament and of The Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts' COM/2021/206 final.

[185] Commission, 'Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC' COM/2020/825 final (DSA proposal), art 31(2).

[186] Zohar Efroni and others (n 178) 19, fn24

[187] On this point, Zohar Efroni and others (n 178) argue that '[f]airness requirements under Chapter III are not limited to SMEs upon which the terms have been unliterally imposed.' ibid, 19.

[188] Josef Drexl and others (n 176) para 127.

There are ambiguities also as to the applicability of Chapter III to Articles 3 and 4. Considering Articles 8(1) and 12 (1), one would conclude that Chapter III does not apply to Articles 3 and 4 of the proposal, which deals with the access right of IoT devices/service users. As Picht puts:[189]

> The obligation to implement FRAND access terms pursuant to Art. 8(1) Data Act ... mentions only access granted to data recipients under Art. 5 Data Act and, e contrario, the reference to "other Union law" can hardly encompass access granted to users pursuant to Art. 3, Art. 4 Data Act.

The position statement of Max Planck Institute argues that the reason for excluding Article 3 and 4 is to make the compensation in Article 9 applicable only to Article 5 since, under Article 4(1), the user of an IoT product shall be able to access and use the data free of charge.[190] However, on this point, Article 12(2) gives rise to second thoughts. The provision reads as: 'Any contractual term in a data sharing agreement which, to the detriment of one party, or, where applicable, to the detriment of the user, excludes the application of this Chapter, derogates from it, or varies its effect, shall not be binding on that party.' The provision defines a larger scope by using the term 'data sharing agreement' and by omitting formerly used terms 'data holder' and 'data recipient' as well as by including the term 'user'. In particular, reference to the 'user' creates ambiguity whether provision intends to include the right of access granted to the users of IoT devices/services in Chapter II.

Regarding the fairness test in Article 13, primary criticism goes to the limited scope confined to SMEs—excluding larger businesses and natural persons not engaging in commercial activity.[191] This is because the imbalance in the bargaining power is not determined by the size of the enterprise but rather the economic dependence of the recipient party on the particular data.[192] The fairness test in Article 13 triggers further questions concerning the interpretation of the wording 'gross deviation from good commercial practice or terms that are contrary to good faith'. It could be expected that there will be a certain period of uncertainty until courts or other relevant authorities establish sufficient interpretative guidance.

The reversed burden of proof in Article 13(5) could be criticised for it requires the proof of a negative fact—that is, the recipient had not attempted to negotiate the allegedly unfair contract term. Such type of requirements makes the discharge of the burden of proof almost impossible. It is also questionable whether it is the best solution to prescribe the lack of recipient's attempt to negotiate the contract as a condition to treat the terms as unilaterally imposed. Where the contract clauses are imposed through a click-wrap license or coded into the technical architecture, this will eliminate the possibility of negotiation and thus keep such terms out of the scope of Article 13.[193]

---

[189] Peter Georg Picht,, 'Caught in the Acts: Framing Mandatory Data Access Transactions Under the Data Act, Further EU Digital Regulation Acts, and Competition Law' (2022) Max Planck Institute for Innovation & Competition Research Paper No. 22-12, 21 <https://ssrn.com/abstract=4076842> accessed 10 October 2022.

[190] Josef Drexl and others (n 176) para 98.

[191] It is a further question of research whether applying the unfairness test to a broader group of data recipients, including consumers (that is, natural persons not engaged in an economic activity) and larger enterprises, could contribute to the goals of the Data Act. See Zohar Efroni and others (n 178) 20-21.

[192] Josef Drexl and others (n 176) para 125.

[193] This additional requirement of 'attempt to negotiate' may also give rise to certain strategies of negotiation to safeguard protection under Article 13, turning an attempt to negotiate into a formality. In practice, such requirement may adversely affect less well-informed small businesses, which are more likely to overlook the requirement before entering into the contract. ibid, para 124.

A further point that raises questions is the lack of any provisions regarding the legal consequences of the presumption of unfairness in Article 13(4). Conventionally, a legal presumption allows the legal acceptance of a particular set of facts as 'true' until certain counter-evidence (which disproves or outweighs the presumed fact) is brought. In this respect, the proposed Act provides no guidance how the presumption of unfairness in Article 13(4) could be rebutted. It is possible that member State procedural laws may differ to a significant extent on this matter.

The proposal repeatedly refers to trade secrets in various provisions stating that appropriate measures shall be taken to preserve the confidentiality of the trade secrets. However, these references provide almost no guidance about how the provisions of the Data Act proposal relating to access or sharing of data will be applied to cases where the data question contains or constitutes a trade secret.

## 7. Chapter V of the Data Act - What is the European concept of "B2G data sharing" in the Data Act proposal? - Antoine Petel[194]

The concept of 'B2G data sharing' is seen as having a high potential for improving public policies.[195] However, this concept is not always defined with the needed clarity in EU Law. To partially address these issues, The European Commission has published the Data Act proposal to specify and harmonise the rules of the 'B2G data sharing' concept.

The concept of 'Business-to-Government (B2G) data sharing' refers to data exchanges from the private sector (such as enterprises and associations) to the public sector (central or local administrations, cities, regions, among others). Under the concept, the Data Act proposal aims to mandate the making available of private sector data to public authorities when the latter is faced with a public interest-related need for such data. A recent example of 'B2G data sharing' is the use of anonymised mobile data from private operators by the EC to monitor the adherence to lockdown measures and anticipate the evolution of the pandemic in Europe.

The 'B2G data sharing' concept is also one of the four European data sharing concepts developed by the European Union to give structure to the European data economy (the three others are the 'B2B', the 'Government-to-Business – G2B', and the 'Government-to-Government – G2G' data sharing – see the Communication 'A European strategy for data').[196]

The Data Act proposal[197] published by the EC in February 2022 introduced the first cross-sector 'B2G data sharing' obligations into EU Law.[198]

### 7.2. What are the obligations of the 'B2G data sharing' concept?

[194] Université Jean Moulin, France.

[195] Commission, High-Level Expert Group on Business-to-Government (B2G) data sharing, 'Final report "Towards a European strategy on business-to-government data sharing for the public interest"' (2020) <https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=64954> accessed 10 October 2022.

[196] Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: "A European strategy for data" COM(2020) 66 final.

[197] 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 (Data Act proposal).

[198] See Data Act proposal, arts 14-22.

First, the Data Act proposal allows public authorities ('public sector bodies' and EU entities) to request data from a 'data holder' (who cannot be a 'small and medium-sized enterprise').[199]

On the one hand, the 'public sector bodies' are 'national, regional or local authorities of the Member States, and bodies governed by public law of the Member States, or associations formed by one or more such authorities or one or more such bodies' (see article 2 (9)). This definition is comprehensive and could embrace, for example, administrations, universities, research organisations, associations, or even possibly enterprises.[200] The EU entities are the institutions (such as the EC, the European Parliament, the European Central Bank, or the European Court of Justice), the agencies (like the European Space Agency and the European Medicines Agency) and the bodies (for example, the European Data Protection Supervisor and the European Investment Bank). On the other hand, the 'data holder' can simply be defined as a legal or natural person who has the right or obligation, under the Data Act proposal, to make available certain data (for the exact definition, see article 2 (6)).

The Data Act proposal enables public authorities to ask for 'B2G data sharing' in case of 'exceptional need'. There is an 'exceptional need' where the data requested is necessary to respond to a 'public emergency' (see article 2 (10)), but also to prevent it or to assist in its recovery. For example, this situation could be a pandemic, a major cybersecurity incident or a natural disaster. There is also an 'exceptional need' where the lack of available data prevents public authorities from fulfilling 'a specific task in the public interest that has been explicitly provided by law' (see also 'B2G data sharing for smart city development in Europe: a first look at the Data Act Proposal').

Moreover, the Data Act proposal imposes different conditions and modalities to protect the data requested. The data cannot be used for another purpose than the one for which it has been requested. It can also not be re-used on the basis of the Open Data Directive (EC) n° 2019/1024.[201] In the same way, public authorities must protect, where applicable, personal or confidential data. If the data requested is no longer needed, it must be destroyed.

## 7.3. What are the issues with the 'B2G data sharing' concept in the Data Act proposal?

The development of the 'B2G data sharing' concept raises many questions, four of them are analysed here.

**1)** Firstly, its scope and obligations shall be clarified in several respects. For example, the definition of 'data holder' (see article 2(6)) seems to include public sector entities. This means that the 'B2G data sharing' framework could apply between public sector entities. Such definition implies therefore a risk of overlap between the 'B2G' and the 'G2G' data sharing. Another example is the ban on further re-use of data made available under the Open Data Directive (EC) n° 2019/1024. However, the Data Act

[199] Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises [2003] OJ L 124/36.

[200] Such as C-360/96 *Gemeente Arnhem and Gemeente Rheden v BFI* Holding [1998] ECR I-06821, para 44.

[201] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (recast) [2019] OJ L 172/56.

proposal does not clarify whether a similar logic applies to data made available for re-use under the 'Data Governance Act'.[202]

**2)** Secondly, the 'B2G data sharing' concept should be differentiated from the deployment of similar concepts in Member States, for example, with the French concept of 'données d'intérêt général' (data of general interest). On the one hand, the European concept proposes a compulsory and cross-sector framework between private and public sectors. On the other hand, the French concept is mostly based on sectoral and voluntary data sharing, and it exceeds the strict relation between the private and public sectors by including data sharing within the private sector. As a result, the similarity of these concepts could lead to a certain confusion on the interaction between the various laws simultaneously applicable.

**3)** Thirdly, the development of the 'B2G data sharing' concept requires the support of the private sector. However, data is a highly strategic asset for private sector entities, which companies may not be keen on sharing. This calls for strong associated legal and technical safeguards, especially to avoid the further disclosure of trade secrets. However, the Data Act proposal does not require the public sector bodies to be equipped with the necessary legal, technical and human resources to comply with these obligations. It could be relevant to strengthen the safeguards in the Data Act proposal in this manner.

**4)** Finally, the development of the 'B2G data sharing' concept requires support to public authorities, some of them being incapable of complying with the 'B2G data sharing' conditions themselves. For example, a local authority may not be able to get the adequate legal expertise or the technical infrastructure to guarantee the protection of the data requested, especially when personal or confidential data are at stake. Ultimately, the 'B2G data sharing' concept may happen to be implemented solely by the largest authorities despite its relevance for public policies (for example, mobility, health and climate).

## 7.4. Conclusion

In conclusion, the concept of 'B2G Data Sharing' appears to be a useful tool to improve public policies. However, given the identified lacunas, developing 'B2G Data Sharing' obligations in Europe requires more precise definitions than those currently found in the Data Act proposal.

# 8. Chapter V of the Data Act - Which should be the legal basis for B2G data sharing: 'exceptional need' or 'public interest'? - Jingyi Chu[203]

B2G data sharing might be the most controversial part of the newly published Data Act proposal,[204] especially in article 15 where public sector bodies have the right to request data from the private sector. This section investigates current 'exceptional need' issues, and analyses the alternative option,

[202] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 [2022] OJ L 152/1 (DGA).

[203] Visiting researcher at Centre for IT & IP Law (CiTiP), KU Leuven, Belgium.

[204] Francesco Vogelezang, '_Rethinking value in data sharing for B2G in the public interest: What to expect from the upcoming Data Act?' (*Open Future*, 28 Jan 2022) <https://openfuture.eu/blog/rethinking-value-in-data-sharing-for-b2g-in-the-public-interest/>.

'public interest'. Besides this, this section builds upon the discussion about the concept of 'B2G data sharing' in the proposal.[205]

As stated in the title of Chapter 5, 'exceptional need' provides the right for public sector bodies to access data held by the private sector, among other things. Article 15 defines the 'exceptional need' for public sector bodies to request data and lists three possible situations for B2G data sharing:

1) the requested data is necessary to respond to a public emergency (see article 15(a));
2) the requested data is necessary to prevent or assist the recovery from a public emergency (the data should be limited in time and scope) (see article 15(b));
3) the lack of available data prevents the public sector from fulfilling a specific task in the public interest that has been explicitly provided by law (see article 15(c)).

It is important to note that public sector bodies can invoke proven 'public interest' under the strict conditions laid down by article 15(c) when they fail to access the requested data by other means, such as market-based means and new legislative measures (see article 15(c)(1)). Hence, 'public interest' can be regarded as a fallback solution or 'last resort'[206] for mandatory B2G data sharing.

## 8.1. What are the current issues with 'exceptional need'?

Article 15 has received criticism since the promulgation of the proposal. On the one hand, some critics hold that article 15 is an ad hoc approach for data requesting, hence arguing that the narrowly-defined 'exceptional need' fails to create a systemic way for public sector bodies to access business data.[207] On the other hand, businesses reacted negatively to proposed B2G data sharing in the European Commission's consultation process,[208] now arguing that Chapter 5 goes too far and that it may hinder their private interests.[209] This section is not intended to choose between these two positions. Nevertheless, it might be hard to define article 15 as an 'ad hoc approach'. This is because the proposal is without prejudice to existing legislation, which may also provide legal bases for public sector bodies to access business data. For example, Chapter 4 of the DGA stipulates rules about data altruism, which allow voluntary B2G data sharing. In addition, as is discussed below, the content of article 15 also raises concrete issues.

First, it is hard to set the boundaries between response, prevention and recovery of public emergencies. For example, as the Covid 19 pandemic is a public emergency that has lasted for more than two years, it is difficult to distinguish whether the requested data is necessary to combat the pandemic's ongoing stage or prevent other variations of the virus in the future. However, two differences between article 15(a) and (b) make it necessary to correctly identify the legal basis. Firstly,

[205] Antoine Petel, 'Chapter 5 of the Data Act - What is the european concept of "B2G data sharing" in the Data Act proposal?' (*CiTiP Blog*, 21 June 2022) <https://www.law.kuleuven.be/citip/blog/chapter-5-of-the-data-act-what-is-the-european-concept-of-b2g-data-sharing-in-the-data-act-proposal/>.

[206] Athena Christofl and Bert Peeters, 'B2G data sharing for smart city development in Europe: a first look at the Data Act Proposal (Part II)' (*CiTiP Blog*, 31 May, 2022) <https://www.law.kuleuven.be/citip/blog/b2g-data-sharing-for-smart-city-development-in-europe-a-first-look-at-the-data-act-proposal-part-ii/>.

[207] Francesco Vogelezang and Alek Tarkowski, '_Data Act: Business to government data sharing' (*Open Future*, 23 February 2022) <https://openfuture.eu/publication/data-act-business-to-government-data-sharing/>.

[208] See European Commission, 'Data Act & amended rules on the legal protection of databases' <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13045-Data-Act-amended-rules-on-the-legal-protection-of-databases/feedback_en?p_id=24828813> accessed 10 October 2022.

[209] Iryna Susha, Jakob Schiele and Koen Frenken, 'Heat map of business opposition to B2G data sharing for public interest in the EU' (*Support Center for Data Sharing*, 26 April 2022) <https://eudatasharing.eu/news/heat-map-business-opposition-b2g-data-sharing-public-interest-eu>.

the data requested in situations of prevention and recovery should be 'limited in time and scope' under article 15(b), while such a limitation is not required under article 15(a). Secondly, according to article 20, data provided under article 15(a) should be free, while data holders can claim compensation in situations of prevention and recovery under article 15(b), including basic costs and a reasonable margin. It might be inevitable to look at the specific case of the request for data sharing in practice. Nevertheless, the unclear boundaries would complicate the required limitations for requested data and the implementation of compensation.

Second, 'public interest' is a broad concept, and the proposal does not give clear interpretational guidelines, which may impede consistent understanding with other legislation. One could wonder whether the notion of 'public interest' under the proposal relates to that enshrined in the GDPR and, if so, how. As noted by Mészáros and Ho,[210] the GDPR has set up different levels of 'public interest', namely, the perceived lower level of 'public interest' (see article 6(1)(e)), the middle level of 'important grounds of public interest' (see article 28(3)(a)), and the higher level of 'substantial public interest' (see article 9(2)(g)). Also, different levels of 'public interest' would lead to different meanings of 'public interest'. For example, GDPR Recital 46 mentions examples of 'important grounds of public interest', which is 'humanitarian purposes, including for monitoring epidemics and their spread or in situations of humanitarian emergencies, in particular in situations of natural and man-made disasters'. As a result, it raises the question of where the “public interest” of the proposal should be located at the different levels.

## 8.2. Would it be a good option to replace 'exceptional need' with 'public interest'?

The Expert Group on B2G Data Sharing 2020 Report regards 'public interest' as the cornerstone[211] of B2G data sharing and broadly refers to it as 'general welfare' or 'the welfare of individuals in society'.[212] Supporters of the “public interest” option suggest replacing “exceptional need” with a clearly defined “public interest”. Instead of playing as a fallback rule, they argue that public sector bodies could use “public interest” proactively. Thus, when the data sharing requests meet the public interest definition (or pass the public interest test), the requested data could be made available.[213] This option would give a stronger mandate for public sector bodies to access business data. Along with supporting and opposing voices, this option could be problematic in implementation because of the broad and context-based definition of ‘public interest’.

Apart from the problems of consistent interpretation, ‘public interest’ is a context-specific and dynamic concept that needs further clarification to make it workable. Additionally, ‘public interest’ is

[210] János Mészáros and Chih Hsing Ho, ‘Big data and scientific research: The secondary use of personal data under the research exemption in the GDPR’ (2018) 59 Hungarian J. Leg. Stud., 403, 408.

[211] Martina Barbero, ‘The Data Act: Opening the door to compulsory B2G data sharing in Europe?’ (*Global Partnership for Sustainable Development Data*, 14 July 2021) <https://www.data4sdgs.org/blog/data-act-opening-door-compulsory-b2g-data-sharing-europe>.

[212] European Commission, Directorate-General for Communications Networks, Content and Technology, ‘Towards a European strategy on business-to-government data sharing for the public interest: final report prepared by the High-Level Expert Group on Business-to-Government Data Sharing’ Publications Office (2021) 16 <https://data.europa.eu/doi/10.2759/731415>.

[213] Alek Tarkowski, Paul Keller, Francesco Vogelezang and Jan. J. Zygmuntowski, ‘_Public data commons: A public-interest framework for B2G data sharing in the Data Act’ (*Open Future*, 24 May 2022) <https://openfuture.eu/publication/public-data-commons/>.

a political concept that needs to be translated into a legal one.[214] As the Expert Group Report indicates, the translation process or the definition of its exact boundaries heavily depends on socio-economic, cultural and historical factors. Therefore, different member States may have different notions of 'public interest', which leads to different spaces for mandatory B2G data sharing. As a result, diverging implementations and forum shopping may happen.

In general, it is therefore not a good option to replace 'exceptional need' with 'public interest'. If the legal grounds for B2G data sharing were to relate directly to "public interest" (that is, instead of the notion of 'exceptional need'), the above shortcomings would be exaggerated. The attempt to give a precise and consistent interpretation is complex and will largely depend on Member States and the CJEU. In contrast, 'public interest' in article 15(c) is a fallback condition, which could largely limit the scope of its application to maintain legal certainty and foreseeability. Moreover, in order to overcome the above shortcomings of this notion, it is crucial to establish a transparent process[215] to identify the concrete 'public interests' and safeguards to prevent public sector bodies from power abuse.

## 8.3. Conclusion

In conclusion, both 'exceptional need' and 'public interest' standards will face implementation difficulties in practice. This section suggests clarifying the connections between the three situations listed in article 15. Given the close relationship between response, prevention and recovery of public emergency, it might be worth reconsidering the differences in the respective legal regimes (in other words, the requirement of 'limited in time and scope' of requested data in article 15(b) and compensation in article 20). Further, since 'public interest' is broad, context-based and political in essence, 'exceptional need', as in the Data Act proposal, appears to constitute a better option as a fallback solution. Thus, when there are no alternative means to access the requested data (in other words, purchasing on the market, relying on existing obligations and new legislative measures), then 'exceptional need' could be invoked as a last resort. Finally, transparency is crucial in the process of identifying the concrete 'public interest'.

# 9. Chapter V of the Data Act – B2G data sharing for smart city development in Europe – Bert Peeters[216] and Athena Christofi[217]

Numerous European cities have been implementing smart-city initiatives in the past few decades. These projects leverage Information and Communications Technologies (ICTs) and data to pursue objectives such as better mobility and transport, more efficient urban services, security and environmental protection. Vast amounts of data about city life are needed to this end. However, valuable data is in the hands of not only municipalities and other public authorities but also private entities: contractors, telecom companies, navigation apps, mobility-as-a-service providers, and digital startups. Access to and the ability to use private-sector data and/or data insights could enable local

[214] Julie Baloup, Emre Bayamlıoğlu, Aliki Benmayor, Charlotte Ducuing, Lidia Dutkiewicz, Teodora Lalova, Yuliya Miadzvetskaya, Bert Peeters, 'White Paper on the Data Governance Act' (2021) CiTiP Working Paper, 42-43 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3872703> accessed 10 October 2022.

[215] Heiko Richter, 'The Law and Policy of Government Access to Private Sector Data ("B2G Data Sharing") in German Federal Ministry of Justice and Consumer Protection, Max Planck Institute for Innovation and Competition (eds), *Data Access, Consumer Interests and Public Welfare* (Baden-Baden, Nomos, 2021) , Max Planck Institute for Innovation & Competition Research Paper No. 20-06 <https://ssrn.com/abstract=3594109>.

[216] Researcher at Centre for IT & IP Law (CiTiP), KU Leuven, Belgium.

[217] Doctoral Researcher at Centre for IT & IP Law (CiTiP), KU Leuven, Belgium.

authorities to better fulfil their public interest missions. The socio-economic value of B2G data sharing is particularly high in the (smart) city context. This contribution first provides some context on the importance of data-sharing mechanisms in smart cities. It then examines certain provisions on B2G mandatory data-sharing found in the proposal for a Data Act, looking at them through a smart-city lens. Finally, this contribution contains some reflections on the interplay between the B2G provisions of the Data Act proposal and data protection law.

## 9.1. Current data-sharing practices and their limitations

Though several cities are realising the benefits of smart-city initiatives and the usefulness of private-sector data to this end, local authorities' access to private-sector data is, to date, exceptional and fragmented. The report of the Expert Group on B2G data sharing (B2G Expert Group)[218] noted that sharing happens primarily through contractual, voluntary arrangements and that these collaborations often are pilot projects failing to evolve into more stable and sustainable initiatives.

Focusing on cities and leveraging insights from interviews with local administrations, research by Micheli[219] zoomed in specifically on the city level and the challenges of current sharing practices. For instance, data donorship practices in which companies freely provide data to certain reputable (smart) cities may pose ethical dilemmas. Companies share data as a marketing strategy to help build and trial marketable use cases. Once marketed, however, data and data-driven services are sold to other smaller or less prominent cities. The latter then 'not only […] lag behind in terms of data innovation, but they have also to pay if they want to benefit from a service that other municipalities got at no-cost'. Public procurement of data, another sharing practice, also comes with challenges. Smart cities necessitate vast amounts of data – numerous datasets might thus need to be procured. Faced with pressing economic challenges, local authorities can be reluctant to purchase data. This is especially so given that 'key issues for data quality, such as representativeness, reliability and resolution' often only emerge when data is accessed, after their procurement. Data partnerships and pools where local authorities and companies pool data and co-create smart-city solutions are interesting tools for B2G data sharing, but they also rely on professional networks and may not be equally accessible to all cities.

## 9.2. From voluntary sharing to sharing requirements

Due to the limitations of current sharing practices, the B2G Expert Group recommended that the European Commission explore the creation of an EU-wide regulatory framework to support B2G data sharing. One of the main pillars of the envisaged framework was the requirements for B2G data sharing.[220] EU regulation could impose sharing obligations for 'EU-wide public interest objectives such as environmental protection, cross-border emergencies […] or the delivery of certain public services' as these objectives may warrant stable channels for B2G cooperation. Mandatory EU-wide data sharing could also concern other data, for example, scarce or unique data. The Expert Group considered that Member States and specific sectors could go beyond these minimum rules and mandate B2G data

[218] Commission, High-Level Expert Group on Business-to-Government (B2G) data sharing, 'Final Report "Towards a European strategy on business-to-government data sharing for the public interest"' (2020) <https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=64954> accessed 10 October 2022.

[219] Marina Micheli, '*Public bodies' access to private sector data: The perspectives of twelve European local administrations*' (2022) 27 (2) First Monday <https://firstmonday.org/ojs/index.php/fm/article/download/11720/10600> accessed 10 October 2022.

[220] Commission, 'Towards a European strategy on business-to-government data sharing for the public interest – Final report prepared by the High-Level Expert Group on Business-to-Government Data Sharing' (2020), 43-45.

sharing 'for purposes that are particularly relevant to their national or local priorities', or sectors concerned.

The envisaged framework could benefit local authorities: EU-wide sharing requirements could create a level-playing field for smart-city development in the EU, and the adoption of further obligations by Member States could enable the same for their respective cities. It could create legal certainty and stable arrangements helping smart cities move past isolated pilot projects. By removing the need for complex contractual negotiations, contract drafting and monitoring, more local authorities will likely access private-sector data and experiment with its potential. Citizens would also benefit since smart-city projects aim towards better and more efficient public services.

The European strategy for data[221] published by the European Commission in February 2020 indicated the Commission's desire to explore regulatory action and devise a Data Act that would foster B2G data sharing for the public interest, among other things. The Inception Impact Assessment[222] was followed by a public consultation in which 100 public authorities participated. An overwhelming majority (91%) of the responding public authorities considered EU or national action on B2G data sharing for public interest purposes necessary.[223] In anticipation of the Data Act, among the proposals of key city stakeholders were: i) the recognition of cities as key players in the B2G data-sharing framework; ii) the definition in the regulatory framework of the data categories that ought to be shared; and iii) the definition of the notion of 'public interest', together with city governments, to ensure that local needs and the wide range of public interest missions for local populations entrusted to municipalities are considered.[224]

## 9.3. The Data Act proposal

The legislative proposal for a Data Act includes provisions on making data available to public sector bodies or Union institutions, agencies or bodies. It explicitly mentions (associations of) Member States' regional and local authorities in the definition of public sector body. Municipalities and other bodies active in the smart-city field (like some inter-municipal associations in Belgium) thus clearly fall under its scope and can benefit from B2G data sharing provisions. Since this section is about smart cities, we use 'local authorities' where the proposal refers to a public sector body or a Union body, to render the discussion more concrete.

Nevertheless, the data-sharing requirements imposed by the act are limited. The obligations in articles 14 and 15 revolve around 'exceptional need'. Data holders must indeed make data available to local authorities that demonstrate an exceptional need to use the requested data. However, though where data holders are micro-enterprises, they are exempt from this obligation (Article 14). The circumstances under which an exceptional need is deemed to exist are then set forth in Article 15.

---

[221] Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: "A European strategy for data" COM(2020) 66 final.

[222] Commission, 'Inception Impact Assessment to the Data Act', Ares(2021)3527151, <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13045-Data-Act-amended-rules-on-the-legal-protection-of-databases_en> accessed 10 October 2022.

[223] Commission, 'Public consultation on data act and amended rules on the legal protection of databases – Summary report on the public consultation' (2021) <https://digital-strategy.ec.europa.eu/en/library/public-consultation-data-act-summary-report> accessed 10 October 2022.

[224] Eurocities, '(Data) Act 1 of Business to Government data sharing' (*Eurocities*, 5 August 2021) <https://eurocities.eu/latest/data-act-1-of-business-to-government-data-sharing/>.

## 9.4. Exceptional need to use data

Article 15 of the proposal specifies three circumstances in which an 'exceptional need to use data' can be established, resulting in an obligation for a data holder to make data available. The first two circumstances relate to the existence of a public emergency. Article 15(a) states that an exceptional need exists where data is necessary to respond to a public emergency. In contrast, under 15(b), such need also exists where data is necessary to prevent or assist recovery from a public emergency. The difference is that where a data request is based on 15(b), it should be limited in time and scope.

Article 15(c) then concerns situations where the lack of available data prevents a local authority from fulfilling a specific task in the public interest that has been explicitly provided by law. Local authorities may thus resort to article 15, either because they have authority in relation to public emergencies under national law or due to their specific tasks in the public interests that are provided by law. Examples of emergency circumstances include public health emergencies, emergencies resulting from environmental degradation, or human-induced major disasters.[225] Stakeholders noted that data-sharing under such circumstances was already happening in several cities, for instance during the covid-19 pandemic.[226] Therefore, the provisions on public emergencies could bring more legal certainty but can only be invoked exceptionally and may not change much in practice. Outside of a public emergency, the proposal provides less detail on what could constitute an exceptional need. Recital 57 merely mentions the compilation of official statistics as an example.

## 9.5. Necessity versus lack of available data preventing fulfilment of a task in the public interest

The first difference between article 15(c) of the proposal and articles 15(a) and (b) is the wording used to describe when these articles may come into play. Whereas 15(a) and (b) state that the use of the data should be 'necessary' to deal with a public emergency, 15(c) requires that a 'lack of available data prevents the public body from fulfilling a specific task in the public interest'. This begs the question of whether the Commission intended to set a different threshold for article 15(c).

The wording used in articles 15(a) and (b) is reminiscent of the wording used in article 6(1)(e) of the GDPR, which essentially provides that the processing of personal data by public authorities must be necessary for the exercise of a public task. One could wonder whether 'necessity' in the context of the Data Act proposal should be given the same meaning as in the GDPR. In the context of article 6(1)(e) GDPR, the Court ruled in the *Huber* case that the data processing could be deemed necessary if it allowed public sector bodies to more effectively exercise their public interest tasks.[227] Given the requirement for an 'exceptional need', one might consider that the threshold set by the Data Act proposal should be applied more strictly. However, public sector bodies' use of personal data should also be seen as an 'exception', given the requirement, for instance, of data minimisation.

Another question is whether, by using a different wording in article 15(c) (that is, a lack of available data that prevents fulfilment of a specific task in the public interest), the Commission intended to

[225] 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 (Data Act proposal), rec 57.

[226] Eurocities, 'The European Commission launches its Data Act' (*Eurocities*, 23 February 2022) <https://eurocities.eu/latest/the-european-commission-launches-its-data-act/>.

[227] C-524/06 *Heinz Huber v Bundesrepublik Deutschland* [2008] ECR I-09705.

provide a stricter threshold for access to data under this article. Based on the wording of this provision alone, it could be understood that the lack of data should arguably render fulfilment of the task in the public interest impossible. It is important to note, however, that recital 58 specifies that the public sector body should 'demonstrate that the lack of timely access to and the use of the data requested prevents it from effectively fulfilling a specific task in the public interest'. This could suggest that the requirements for access to data are quite similar to those for public sector bodies to lawfully process personal data.

## 9.6. Article 15(c) as a last resort

Given the clarification of recital 58, demonstrating that the lack of data prevents fulfilling a task in the public interest might not be the most difficult hurdle for local authorities to access data. The additional requirements set by points 1 and 2 of article 15(c) may prove more challenging. To rely on 15(c) local authorities need to demonstrate that:

1) they have been unable to obtain the requested data 'by alternative means including by purchasing the data on the market at market rates or by relying on existing obligations to make data available, and the adoption of new legislative measures cannot ensure the timely availability of the data'; or
2) obtaining the data in line with the procedure laid down in the proposal 'would substantively reduce the administrative burden for data holders or other enterprises'.

Under point 1, local authorities embarking on smart-city initiatives must consider alternative means to access private-sector data. The purchase of 'data on the market and at market rates' is one such means. However, depending on the type of the requested data and its market maturity, this may not be an easy feat. The B2G Expert Group report illustrated the challenge of buying data due to data being an 'experience good'.[228] This means that 'its value is unknown until it has been used for a particular purpose. When used for a different purpose, its value may not be the same, in particular because the real value of data does not come from a single dataset, but from combining datasets from different sources'. Establishing fair smart-city data markets can be a difficult endeavour. Local authorities would need to evidence their inability to purchase data at market rates. How easily this can be done for datasets not readily offered on the market remains to be seen.

Relying on existing obligations to access data is another means that could be considered. Where no such obligations or alternative means of access exist, new legislative measures should be contemplated unless this cannot ensure the timely availability of data. In this sense, article 15(c) is subsidiary to existing (and future) legislative measures requiring data sharing. Arguably, this makes the harmonisation effect of the B2G data-sharing obligations found in the Data Act rather minimal.

Point 2 provides an additional possibility to access private-sector data. Where requesting data access based on the proposal would substantively reduce the administrative burden for data holders or other enterprises, local authorities can base their access request on article 15(c).

[228] Commission, 'Towards a European strategy on business-to-government data sharing for the public interest – Final report prepared by the High-Level Expert Group on Business-to-Government Data Sharing', (2020) 17.

## 9.7. Data Act's interplay with data protection legislation in the case of personal data

As a final point on the Data Act and smart cities, it is important to highlight some potential issues regarding personal data, as many of the private-sector datasets that are useful for local authorities originate from personal data (for example, data from telecom or mobility-as-a-service companies). The proposal qualifies that it is without prejudice to "EU law on data protection and privacy" (recital 7) and that parties to data sharing should implement measures on data minimisation and data protection by design (recital 8). In the eyes of the Commission, EU data protection legislation and new legislation on data sharing are to co-exist.

The proposed solution is generally to impose strict adherence to principles of data minimisation and data-protection-by-design. Indeed, article 17 of the proposal specifies that requests for private-sector data shall 'concern, insofar as possible, non-personal data'. In drafting the proposal, the Commission seems, however, not to have taken account of the critical views expressed by the European Data Protection Supervisor (EDPS) and European Data Protection Board (EDPB) in their Joint Opinion on the Data Governance Act.[229] In their opinion, these bodies stressed that the distinction between personal and non-personal categories of data is very difficult in practice, particularly in cases where 'non-personal data are the result of anonymization of personal data'.[230] Increasing the availability of such data and allowing its re-use and combination with other datasets increases re-identification risks and thus poses challenges for both private-sector bodies and local authorities. Private-sector bodies, for instance, assume a legal risk by sharing datasets of an unclear personal/non-personal data classification.

The risks to citizens' fundamental rights linked to increased availability of data are not clearly addressed in the proposal beyond the confirmation of the data minimisation and proportionality principles. The investments required in processes and mechanisms that allow for a 'lifecycle approach' towards data and adequately addressing possible risks are left entirely to individual local authorities and companies. Without such a 'lifecycle' approach, there is a risk that B2G data-sharing happens in a way that bypasses otherwise essential data protection law requirements such as lawfulness and purpose limitation.

## 9.8. Unclear relationship between Article 15 Data Act proposal and Article 6 GDPR

As the Data Act is without prejudice to existing data protection law, the GDPR principles of lawfulness of processing and purpose limitation are fully applicable to B2G personal data sharing. This brings the question of how Article 15 Data Act proposal interacts with the respective GDPR provisions.

The lawfulness principle requires any processing of personal data (including sharing) to have a valid legal basis. Legal bases are exhaustively listed in Article 6(1) GDPR. As Article 15 Data Act proposal is meant to create an obligation to share (personal) data in certain cases, the GDPR legal basis that best

[229] EDPB-EDPS, 'Joint Opinion 03/2021 on the Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act)' (2021) <https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-032021-proposal_en> accessed 10 October 2022.

[230] Ibid, 16.

matches the situation is the one Article 6(1)(c) provides: processing necessary for compliance with a legal obligation to which the controller is subject. Article 6(3) further specifies that the basis for such processing must be laid down by EU or national law.

Respect for the purpose limitation principle must also be ensured as data sharing certainly constitutes further processing of personal data. Further processing is only allowed for purposes compatible with the initial data collection purpose: in principle, incompatible further processing is prohibited. In the envisaged B2G data sharing, personal data collected for commercial-related purposes are essentially re-purposed for public interest-related ones. There is hardly any link between the two purposes. Rather, a wide change of context would make further processing unexpected for data subjects. The wording of Article 6(4) GDPR suggests that incompatible processing can only proceed if data subjects give their consent to it or if it is based on an EU or Member State law 'which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1)'. Article 23(1) GDPR itself provides an exhaustive list of objectives that include national security, defence and other important objectives of general public interest of the Union or of a Member State.

Considering the above GDPR requirements does the Data Act proposal, especially Article 15 laying down obligations for B2G data sharing, constitute an EU law that can provide a valid legal basis for sharing data and its subsequent use by local authorities? In their joint opinion on the proposal the EDPB and the EDPS consider that they do not.[231] Limitations on the right to data protection not only require a legal basis but one that meets certain 'quality of the law' requirements. The legal basis must be 'accessible and foreseeable and formulated with sufficient precision to enable individuals to understand its scope'. This is even more important, we argue, considering that the sharing and access to data by public authorities constitutes a further interference to the right to data protection. In other words, an interference additional to the one that already happened with the data's first collection and processing.

The joint opinion identifies several weaknesses of Article 15 in that regard. For instance, 'public emergencies' and 'exceptional need' are broadly defined. From the point of view of data subjects, circumstances requiring private operators to share citizens' personal data are imprecise and unforeseeable. The provision also fails to specify the categories of personal data that can be accessed, the safeguards for data subjects, and to clearly delineate the powers of public authorities when accessing the data. In our view, this impacts 'quality of the law' and makes it difficult to assess the measure's necessity and proportionality, even though such assessment is necessary for limitations on fundamental rights according to Article 52(1) of the EU Charter. Overall, the joint opinion calls for the EU legislator to define B2G data sharing with much more precision in the eventual Data Act.

Is it possible for an EU-wide act to specify with sufficient precision all the various elements concerned, such as public interests, public authorities, and personal data categories considering so many EU, national, local and sector-specific interests that may justify B2G data sharing? Or should B2G sharing obligations rather come via sectoral and/or national and sub-national legislation? While the objective of harmonisation is certainly hindered in the second scenario, that scenario does have certain benefits

[231] EDPB, EDPS, 'EDPB-EDPS Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)' 20 (2022).

in terms of fundamental rights (ability to better meet requirements of quality of the law, necessity and proportionality) and legitimacy.

## 10. Chapter VI of the Data Act – The 'right to switching' - Charlotte Ducuing[232]

Chapter VI of the Data Act proposal aims to fulfil the long-standing EC objective to facilitate customers' switching from one cloud (and more recently edge) computing service provider (together 'data processing services') to another and, thereby, restore an acceptable level of competition in such markets.[233] The present section is structured as follows: the first subsection outlines the legal regime proposed by Chapter VI of the Data Act proposal, namely a non-explicit right to switching. It is argued that Chapter VI appears to establish a sui generis legal regime. This raises the question of how it relates to legal mechanisms already known in EU contract law, which is explored in the second subsection. Especially, the relationship to the Digital Content Directive is not fully recognised, which raises questions for private law enforcement. Also, reading the Digital Content Directive helps discern issues concerning the notion of 'functional equivalence'.

This section does not provide an exhaustive analysis of Chapter VI and leaves out the crucial questions of interoperability and standardisation and of its scope. Also, the relationship between Chapter VI and other legal frameworks, such as IP rights, is not discussed.[234]

### 10.1. A non-explicit 'right to switch'

Chapter VI of the Data Act proposal follows the failure ('limited efficacy')[235] of the soft law approach under the Free-Flow of Non-Personal Data Regulation,[236] whereby the European Commission was under the obligation to 'encourage and facilitate the development of self-regulatory codes of conduct' by companies.[237] In contrast, Chapter VI of the Data Act proposal engages decidedly in heavy-hand regulation of data processing service contracts. Without directly and explicitly recognising a 'right to switching',[238] Article 23 mandates data processing service providers to take a set of measures to 'remove obstacles to effective switching between providers of data processing services'.[239] Providers shall 'remove commercial, technical, contractual and organisational obstacles' related to themselves, which currently prevent customers from conducting all the constitutive elements of 'switching'. This

[232] Doctoral researcher at Centre for IT & IP Law (CiTiP), KU Leuven, Belgium.

[233] 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 (Data Act proposal), rec 69.

[234] On issues of scope of application rationae materiae and on the relationship with IP rights, see Simon Geiregat, 'The Data Act: Start of a New Era for Data Ownership?' (2022) sec 3.2 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4214704> accessed 10 October 2022. On the scope of application rationae materiae, see also 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 No. 22-05, paras 169-173 <https://pure.mpg.de/rest/items/item_3388757_4/component/file_3395639/content> accessed 7 October 2022.

[235] Data Act proposal, rec 70.

[236] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union [2018] OJ L 303/59 (Free-Flow of Non-Personal Data Regulation), art 6.

[237] Free-Flow of Non-Personal Data Regulation, art 6(1).

[238] BDVA, 'BDVA position paper Response to the European Commission's proposal for a Data Act' (2022) sec 5 <https://www.bdva.eu/sites/default/files/BDVA%20Position%20paper%20Data%20Act%20-%20v1.0.pdf>, accessed 10 October 2022.

[239] Data Act proposal, art 23, heading.

includes the termination of the contractual agreement, the conclusion of (a) contract(s) with (a) different provider(s), the porting of their applications and digital assets, including data, to the said provider(s) and, finally, the ability for customers to effectively use their assets in the new environment.[240]

To ensure compliance, Chapter VI also provides how switching shall be conducted for both the contractual[241] and the technical[242] aspects. The provider and the customer shall agree on a number of contractual terms stipulating the conditions for switching. Article 25 lays down a gradual withdrawal of switching charges. Technically, switching shall be based on a newly coined principle of 'functional equivalence' in case of 'IaaS' (Infrastructure-as-a-Service), namely

> the maintenance of a minimum level of functionality in the environment of the new [data processing service] after the switching process […] to such an extent that […] the destination service will deliver the same output at the same performance and with the same level of security, operational resilience and quality of service as the originating service at the time of termination of the contract.[243]

In such a case, therefore, switching includes not only a negative obligation not to hinder switching (that is, obligation to 'remove obstacles'). The obligation to provide functional equivalence implies indeed also seemingly a positive obligation of assistance to customers in the IT environment of the new service provider(s) when so doing. This is confirmed by Recital 74, which clarifies that data processing service providers should be required to 'offer all assistance and support that is required to make the switching process successful and effective (…)'.

In all other cases (for example, Software-as-a-Service or 'SaaS'), data processing service providers shall make 'open interfaces publicly available and free of charge' and ensure compatibility with 'open interoperability specifications or European standards for interoperability' to be developed by European standardisation bodies.[244]

The EC could have been clearer in laying down a plain enforceable 'right to switching'.[245] It would also serve to clarify that the service provider appears not to be imposed solely a negative obligation to remove obstacles to switching, as it could seem at first glance, but also seemingly a positive obligation to deliver on switching, including by assisting in the IT environment of the new service provider (namely, a competitor).

## 10.2. Switching under the Data Act vs conformity requirements under the Digital Content Directive

[240] Ibid, art 23 and rec 72.
[241] Ibid, art 24.
[242] Ibid, art 26.
[243] Ibid, art 2(14) and rec. 72.
[244] Ibid, Ch VII and rec 76.
[245] See also BDVA (n 239), sec 5.

In 2019, the EU adopted the Digital Content Directive[246] to harmonise the regulation of related contracts for the benefit of consumers and of the internal market. The Directive also adapts the legislative framework to the digital environment. Where provided as a stand-alone service to consumers,[247] data processing services constitute 'digital services' governed by the Digital Content Directive.[248] The trader shall notably supply services that meet both 'subjective' and 'objective' requirements for conformity, as defined under the Directive.[249] As part of the 'objective requirements for conformity', data processing services shall be 'fit for the purposes for which digital content or digital services of the same type would normally be used, taking into account, where applicable, any existing Union and national law (…)'.[250] This provision seems to create a broad scope for obligations in other legislations to qualify as conformity requirements. Should switching be considered as an inherent part of the object of data processing services following the Data Act, it raises the question of how switching-related obligations can be squared with the regulation of conformity requirements under the Digital Content Directive, when provided to consumers. The ambitious way in which switching is conceived of, meaning the obligation to provide assistance services in the IT environment of the new provider, as discussed above, reinforces the relevance of this question.

This issue is, however, not addressed in the Data Act proposal, which refers to the Digital Content Directive seemingly only to confirm that Chapter VI of the Data Act is without prejudice to the rights of consumers upon termination of contracts, as granted by the Digital Content Directive.[251] This consideration is, of course, welcome - even though further clarification would be advisable.[252] Still, this would seem to imply that, a contrario, switching-related obligations have nothing to do with conformity requirements. As regulated under the Data Act, switching would then only constitute a specific modality for data processing contract termination. However, such an interpretation stands in sharp contrast to the wording of the Data Act (see above subsection) and shall be discarded. Our

[246] Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services [2019] OJ L 136/1 (Digital Content Directive). The Digital Content Directive was adopted together with the Sales of Goods Directive, Directive (EU) 2019/771 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the sale of goods, amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC [2019] OJ L 136/28 (Sales of Goods Directive). The Sales of Goods Directive applies to the sale of tangible products, including when accompanied by digital elements. On the scope of the respective directives, see Hugh Beale, 'Digital Content Directive And Rules For Contracts On Continuous Supply' 2021 12 (2) JIPITEC <http://www.jipitec.eu/issues/jipitec-12-2-2021/5286> accessed 10 October 2022; Paula Giliker, 'Regulating Contracts for the Supply of Digital Content: The EU and UK Response' in Tatiana-Eleni Synodinou, Philippe Jougleux, Christiana Markou and Thalia Prastitou (eds), *EU Internet Law* (Springer, 2017), 101–24 <https://doi.org/10.1007/978-3-319-64955-9_5; Karin Sein, 'What Rules Should Apply to Smart Consumer Goods?

[247] Or, more generally, when neither embedded with a tangible good, nor interconnected or ancillary to a tangible good within the meaning of the Digital Content Directive, art 3(4) (and rec. 21 and 22), and the Sales of Goods Directive, art 3(3) (and rec. 13, 15 and 16). On the difficult delineation between the scope of application of the respective directives, see Sein, 'What Rules Should Apply to Smart Consumer Goods? Goods with Embedded Digital Content in the Borderland Between the Digital Content Directive and "Normal" Contract Law'; Karin Sein, 'The Applicability of the Digital Content Directive and Sales of Goods Directive to Goods with Digital Elements' 2021 30 Juridica International <https://doi.org/10.12697/JI.2021.30.04> accessed 10 October 2022.

[248] A digital service is defined as either (a) a service that allows the consumer to create, process, store or access data in digital form; or (b) a service that allows the sharing of or any other interaction with data in digital form uploaded or created by the consumer or other users of that service", Digital Content Directive, art 2(2). See also rec 19.

[249] Digital Content Directive, art 6.

[250] Ibid, art 8(1)(a).

[251] Art 24(1) reads: "The rights of the customer and the obligations of the provider of a data processing service in relation to switching between providers of such services shall be clearly set out in a written contract. Without prejudice to Directive (EU) 2019/770, that contract shall include at least the following […]". Recital 74 reads: "Existing rights relating to the termination of contracts, including those introduced by [the Digital Content Directive] should not be affected".

[252] Josef Drexl and others, (n 235) para 177.

understanding is that switching, as regulated under the Data Act, constitutes a service that shall be provided to customers as part of data processing services, leading to the termination of the contract. Conformity requirements under the Digital Content Directive should thus logically and automatically apply to switching, without needing further reference in the Data Act.

However, the regulation of conformity requirements in the Digital Content Directive, namely the consequences in case of breach, does not quite fit the specificities of switching. Switching takes place partly in the IT environment of a third party, namely the new service provider, and it requires a form of exchange and cooperation between the original and the new service providers. Switching implies, therefore, a triangular relationship, while the Digital Content Directive envisages mainly bilateral relationships, namely between the trader and the consumer.[253] For example, the Digital Content Directive valuably regulates the legal consequences of a lack of conformity resulting from the incorrect integration of the digital content or service into the consumer's digital environment[254] but not into a third party's (namely the new service provider's) environment. Similarly, neither the liability provision (Article 11) nor the burden of proof provision (Article 12) considers the role of the new service provider in the smooth operation of switching. Finally, the gradual withdrawal of switching charges (as part of Article 25 of the Data Act) may have undesirable consequences on the application of Article 14 of the Digital Content Directive (remedies for lack of conformity).

To conclude, the relationship with the regulation of conformity requirements under the Digital Content Directive has been seemingly overlooked. It is recommendable, first, to expressly regulate whether switching is subject to conformity requirements. Should it be the case, as our analysis finds, it is necessary to regulate the specificities of switching, especially the role of the new service provider and of its IT environment, as a lex specialis to the Digital Content Directive.

## 10.3. The notion of 'functional equivalence' under the Digital Content Directive

In this subsection, it is argued, first, that the relationship between the notion of 'functional equivalence' under Chapter VI of the Data Act and this of 'functionality' under the Digital Content Directive shall be clarified. Second, the obligation to provide 'functional equivalence' raises interpretation questions, made visible thanks to the distinction between 'subjective' vs 'objective' conformity requirements in the Digital Content Directive.

Both the Digital Content Directive and the Data Act refer to functionality. In both cases, functionality serves as a yardstick to evaluate whether the quality of the service is acceptable. However, functionality is not conceptualised in the same manner.

As a reminder, the Data Act proposal defines 'functional equivalence' as 'the maintenance of a minimum level of functionality in the environment [of the new provider] after the switching process (…)' (see section 10.1).[255] According to Recital 74, service providers shall not be required to

[253] The Digital Content Directive does consider third parties in certain instances, such as with Art. 10 concerning third-party rights.
[254] Digital Content Directive, art 9.
[255] Data Act proposal, art 2(14).

> develop new categories of services within or on the basis of the IT-infrastructure of different data processing service providers to guarantee functional equivalence in an environment other that they own systems. Nevertheless, service providers are required to offer all assistance and support that is required to make the switching process effective.[256]

In turn, the Digital Content Directive uses the notion of 'functionality', defined as 'the ability of the digital content or digital service to perform its functions having regard to its purpose'.[257] Functionality has then two dimensions: it constitutes both an objective requirement, considered against the yardstick of 'digital content or digital services of the same type and which the consumer may reasonably expect (…)' (emphasis added)[258] and a subjective requirement, the latter being - logically - relative to the contractual commitments of the trader.[259]

Against this background, two separate questions can be raised, to which no satisfactory answer can be found in the Data Act proposal. First, does the obligation for the provider to ensure 'functional equivalence' after the switching process in the IT environment of the new provider according to the Data Act proposal relate to 'functionality' as per the Digital Content Directive, or should it be interpreted independently from the former?

Second, does the notion of 'functional equivalence' encompass only an *objective* dimension or also a subjective one, whether by reference to the notion of 'functionality' as per the Digital Content Directive or independently from it? In other words, against which yardstick should the functional equivalence be evaluated? This question is of particular significance for both the efficacy and the feasibility of Chapter VI of the Data Act. While there is a variety of data processing services, especially cloud computing ones, in some instances it may be crucial for customers to be able to rely on specific functionality requirements agreed with the original provider (that is, where cloud computing services are safety-critical). On the other hand, and subject to further business and technical analysis, requiring the original provider to ensure a functional equivalence concerning specific contractual commitments may prove particularly challenging if the IT environment of the new provider does not allow for such features. The statement, in Recital 74, that the original provider does not have to develop new categories of services within or on the basis of the IT-infrastructure [sic] of the new service provider, does not answer this question.

To conclude, it is recommendable to clarify the relationship of ‘functional equivalence’ with ‘functionality’ under the Digital Content Directive. The question of whether the Data Act should embrace an all-encompassing ‘functional equivalence’ concept (including both objective and subjective elements) is for policymakers to decide. However, should they opt for such a far-reaching option, they may want to reconsider the imposition of switching free of charge in the medium term.[260] Besides, this discussion highlights again the need for clear provisions on the circumstances in which the integration in the IT environment of the new provider may exonerate the original provider of the

[256] Ibid, rec 74.
[257]Digital Content Directive, art 2(11).
[258] Ibid, art 8(1)(b).
[259] Ibid, art 7(a).
[260] Data Act proposal, art 25(1).

switching-related obligations. The original provider should not have to vouch for the new provider('s IT environment).

## 11. Chapter VII – New rules to govern non-EU/EEA governments access to and transfer of non-personal data. Some insights and recommendations - Maria Avramidou[261]

One of the core objectives of the Data Act proposal is to establish safeguards against unlawful non-personal data access by and transfers to third countries without notification by cloud service providers.[262] The aim of such safeguards will be to further enhance trust in the data processing services, including cloud services, that increasingly underpin the European data economy. These rules are an important step towards the establishment of such safeguards. Nevertheless, some elements of the relevant rules are still broad or unclear and would benefit from amendment and further clarification.

Chapter VII of the Data Act addresses, among others, the unlawful third-party access to and transfer of non-personal data held in the European Union by data processing services, including cloud services, offered in the EU market.[263] It provides for specific safeguards, based on which cloud service providers must take all reasonable measures to prevent such access or transfer when it conflicts with competing obligations to protect such data under EU law, unless the conditions set on the Data Act proposal are met (see the analysis below). Until now, access to and transfer of non-personal data to third countries were not regulated. However, with the adoption of the DGA and the Data Act proposal, such access and transfer will be regulated at EU level.[264]

Article 27 of the Data Act proposal requires providers of data processing services, namely cloud and edge service providers, to deploy all reasonable technical, legal and organisation measures in order to prevent the transfer to third countries (that is, transfer of data outside the EU) or governmental access to non-personal data that would violate EU or national law.[265] Moreover, any decision or judgment of a court or tribunal and any decision of an administrative authority of a third country that requires a provider of data processing services to transfer from or give access to non-personal data within the scope of the Data Act proposal held in the EU may only be recognised or enforceable in any manner if based on an international agreement such as a mutual legal assistance treaty.[266] In the absence of such an agreement, where a provider of data processing services is the addressee of such a decision or judgment of a court, tribunal or administrative authority of a third country ordering the transfer of or access to non-personal data within the scope of the Data Act proposal held in the EU; and when compliance with such a decision or judgement would risk putting the addressee in conflict with EU law

[261] Centre for IT & IP Law (CiTiP), KU Leuven, Belgium.

[262] 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 (Data Act proposal).

[263] Data Act proposal, Ch VII.

[264] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 [2022] OJ L 152/1 (DGA); See for instance Julie Baloup, 'Data Act Chapter VII: New rules to govern non-EU/EEA governments access to and transfer of non-personal data (*CiTiP blog*, 23 June 2022) <https://www.law.kuleuven.be/citip/blog/data-act-chapter-vii-new-rules-to-govern-non-eu-eea-governments-access-to-and-transfer-of-non-personal-data/>.

[265] Data Act proposal, art 27, para 1.

[266] Ibid, art 27, para 2.

or with the national law of the relevant EU Member State, transfer of or access to such data by that third-country authority shall take place only if the following conditions are fulfilled, cumulatively:

a. The Non-EEA (European Economic Area) country system requires the reasons and proportionality of the decision or judgement, which is specific, for example, by establishing a sufficient link with certain suspected persons or infringements;

b. The addressee of the order can request the review of that decision or judgement by a competent court or tribunal;

c. The competent court or tribunal issuing the decision or judgement or reviewing the decision of an administrative authority is empowered under the law of that country to take duly into account the relevant legal interests of the provider of the data protected by Union law or national law of the relevant Member State.[267]

In case neither an international agreement is in place, nor the conditions under a-c are met, the addressee of the access/transfer request should not provide access or transfer the data at hand. In the process of examining whether the conditions of Article 27 of the Data Act proposal are met, especially in situations of commercially sensitive data, meaning data that its disclosure could jeopardise the addressee's commercial interests, or when national security or defence interests are at stake, the addressee may request the opinion of a competent body or authority.[268] Moreover, when there is either an international agreement or the conditions a-c listed above are met, the addressee of the access/transfer request must provide only the minimum permissible amount of data;[269] and should notify the data holder for such request, except when the request at hand serves law enforcement purposes and such notification would jeopardise the effectiveness of the law enforcement activity.[270]

It can be argued that the term 'all reasonable measures' is too broad and can create uncertainty in its practical implementation.[271] Thus, it can be suggested to replace the term 'all reasonable measures' with 'all reasonably foreseeable measures'. With this amendment, only the measures that are foreseeable at the day and age of their implementation will serve as the criterion for compliance, thereby narrowing down the available reasonable measures and at the same time allowing for the future-proofness of the provision. An alternative could be the suggestion of the European Data Protection Supervisor and the European Data Protection Board in their Joint Opinion 02/2022 to either remove the term 'reasonable' or replace it with a term such as 'necessary' in order to ensure the efficiency of the measures at hand.[272] Nevertheless, the term 'all reasonable measures' can be maintained in the Data Act in order to ensure consistency with the recently adopted Data Governance Act, and to avoid further possible interpretation challenges.

---

[267] Ibid, art 27, para 3.

[268] Ibid, art 27, para 3.

[269] Ibid, art 27, para 4.

[270] Ibid , art 27, para 5 and art 2 (6). The term 'data holder means 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'.

[271] See for instance also, Julie Baloup, Emre Bayamlıoğlu, Aliki Benmayor, Charlotte Ducuing, Lidia Dutkiewicz, Teodora Lalova, Yuliya Miadzvetskaya, Bert Peeters, 'White Paper on the Data Governance Act' (2021) CiTiP Working Paper <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3872703> accessed 10 October 2022.

[272] EDPB, EDPS, 'EDPB-EDPS Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)' (2022).

In addition, Article 27 of the Data Act proposal does not specify the consequences of the opinion of the competent body or authority on whether the conditions for non-personal data access/transfer are fulfilled and its nature as binding or not. In this context, it should be clarified whether, in case such an opinion concludes that these conditions are not met, the addressee of the request is obliged not to grant access to or transfer that data. In case such an opinion is not binding, it should be further clarified whether the addressee of the access/transfer request should justify their decision to deviate from that opinion.

To conclude, the rules of Article 27 of the Data Act proposal are an important step towards the establishment of safeguards against unlawful data access by and transfer to third countries without notification by cloud service providers. Nevertheless, to better enhance the Data Act proposal, it is suggested that the term 'all reasonable measures' could be replaced with the term 'all reasonably foreseeable measures' or the term 'necessary'. Moreover, it should be clarified whether the opinion of the competent authorities or bodies on whether the conditions of Article 27 of the Data Act proposal are met should be binding or not.

## 12. Chapter VII of the Data Act – GDPR-like rules imposed on cloud services providers regarding protected non-personal data - Julie Baloup[273]

With Article 27 of the Data Act proposal, the European Commission introduces new rules to govern international transfers of and access to non-personal data held in the EU by providers of data processing services. In particular, these new rules aim to apply to international transfers of and access to data protected by IP and trade secrets upon request of non-EU/EEA governments.

These new rules, directly imported from the Data Governance Act,[274] complement the GDPR[275] with the aim to elaborate a comprehensive legal framework for international access to and transfer of data, particularly in the context of requests of foreign governments for law enforcement purposes. Against this background, this section aims to give an overview of the future EU regulatory landscape in relation to data transfer and access requests by foreign governments while drawing attention to potential issues relating to its application.

### 12.1. State of play - International transfers of data on request by non-EU/EEA governments

When it comes to international transfers of data, the focus has mainly been on personal data so far to preserve individuals' right to personal data protection under the EU Charter (Article 8), especially based on the GDPR. In that regard, Article 48 GDPR lays down strict rules for international transfers in

[273] European Commission, Belgium.

[274] See Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 [2022] OJ L 152/1 (DGA), art 31.

[275] See Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L 119/1 (GDPR), art 48.

response to requests by non-EU/EEA governments for law enforcement and other legitimate purposes.[276]

In contrast, no statutory provisions regulating international transfers of non-personal data are currently in force. This is about to change. The Data Governance Act,[277] which was adopted on 30 May 2022 and will be in force as from 24 September 2023, lays down GDPR-like rules to govern:

**1)** international transfers initiated by re-users of non-personal data covered by third parties' rights that are held in public databases (Article 5);[278] as well as

**2)** international access to or transfers of non-personal data protected by third parties' rights, in particular in the context of transfers or access requests by non-EU/EEA governments addressed to data sharing intermediaries and re-users of data held in public databases[279] (Article 31).[280]

The rights and interests of holders of data covered by IP rights and trade secrets may be jeopardised in case of disproportionate access or transfer requests by non-EU/EEA governments addressed to providers of data processing services, such as cloud services providers, processing their data in the EU. The absence of regulation of such transfers is problematic as, like an individual's right to personal data protection, rights of holders of data covered by IP rights or trade secrets are protected under the EU Charter's rights to property (Article 17) and to conduct a business (Article 16). The Data Act aims to rectify this situation.

## 12.2. In the future – Safeguarding the rights and interests of cloud services providers' clients in the context of access or transfer requests by non-EU/EEA governments

The Data Act introduces GDPR-like rules to govern international transfers of non-personal data held by cloud service providers, including transfers of and access to data protected by IP rights or trade secrets in the context of access or transfer requests by non-EU/EEA governments.

In particular, the Data Act mandates providers of data processing services to 'take all reasonable technical, legal and organisational measures, including contractual arrangements' to prevent transfer

[276] Article 48 GDPR on Transfers or disclosures not authorised by Union law states that 'Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter.'

[277] DGA.

[278] For more details, see Julie Baloup, Emre Bayamlıoğlu, Aliki Benmayor, Charlotte Ducuing, Lidia Dutkiewicz, Teodora Lalova, Yuliya Miadzvetskaya, Bert Peeters, 'White Paper on the Data Governance Act' (2021) CiTiP Working Paper, 15-26 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3872703> accessed 10 October 2022. See also Julie Baloup, 'The Data Governance Act: New rules for international transfers of non-personal data held by the public sector' (*European Law Blog*, 10 June 2021) <https://europeanlawblog.eu/2021/06/10/the-data-governance-act-new-rules-for-international-transfers-of-non-personal-data-held-by-the-public-sector/>.

[279] Article 31 of the DGA states 'The public sector body, the natural or legal person to which the right to re-use data was granted under Chapter II, the data intermediation services provider or the recognised data altruism organisation shall take all reasonable technical, legal and organisational measures, including contractual arrangements, in order to prevent international transfer or governmental access to non-personal data held in the Union where such transfer or access would create a conflict with Union law or the national law of the relevant Member State, without prejudice to paragraph 2 or 3'.

[280] For more details see Julie Baloup and others (n 279) 51-53.

of or deny access to non-personal data held in the EU where such a transfer or access would create a conflict with EU law or national law of a Member State.[281] In practice, regarding requests by foreign governments, this implies that similarly to the mechanism under Article 48 GDPR, transfers will have to be blocked and access denied unless based on an international agreement such as a mutual legal assistance treaty.[282]

Alternatively, the transfer or access may only happen provided that the third country offers sufficient rule of law guarantees. In particular, transfer to or access to such data by that third-country authority shall take place only:

> (a) where the third-country system requires the reasons and proportionality of the decision or judgement to be set out, and it requires such decision or judgement, as the case may be, to be specific in character, for instance by establishing a sufficient link to certain suspected persons, or infringements;
>
> (b) the reasoned objection of the addressee is subject to a review by a competent court or tribunal in the third country; and
>
> (c) the competent court or tribunal issuing the decision or judgement or reviewing the decision of an administrative authority is empowered under the law of that country to take duly into account the relevant legal interests of the provider of the data protected by Union law or national law of the relevant Member State.[283]

To assess whether the third country offers sufficient rule of law guarantees, the Data Act proposal provides for the possibility for the addressee of the decision to ask the opinion of

> the relevant bodies or authorities (…) in order to determine whether those conditions are met, notably when it considers that the decision may relate to commercially sensitive data, or may impinge on national security or defence interests of the Union or its Member States.

While this is only a possibility, it is also unclear from the text what would be the legal value of such an opinion. In addition, this mechanism will likely be abandoned in the adopted version of the text, following the path of the DGA for which political negotiations resulted in adopting a self-assessment approach, deleting the reference to any institution's opinion on this matter. This would mean that providers of data processing services would be left with the responsibility to decide, in the absence of a relevant international agreement, whether foreign governments requesting access to or transfer of the clients' data provide sufficient rule of law guarantees.

With the introduction of these new rules, the EU complements Article 48 GDPR by creating a comprehensive legal framework that covers both personal data and non-personal data subject to IP rights/trade secrets, while ensuring a high level of IP/trade secrets protection.

---

[281] 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 (Data Act proposal), art 27, para 1.

[282] Ibid, art 27, para 2.

[283] Ibid, art 27, para 3.

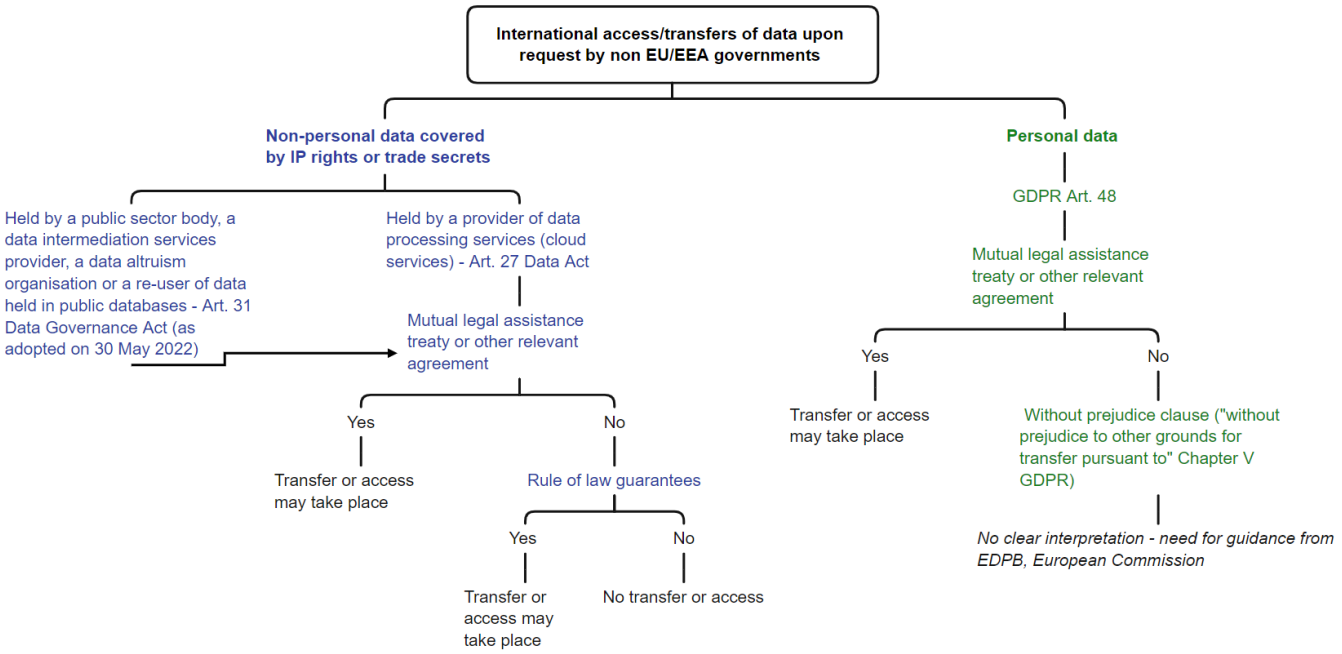


**Fig. 3: International access/transfers of data upon request by non-EU/EEA governments: mapping the future EU regulatory landscape**

## 12.3. Will this be workable?

Three main issues should be considered in the case of foreign government's requests for access or transfer of data addressed to cloud services providers.

First, personal and non-personal data can be mixed in datasets where IP/trade secret protection and data protection may overlap, as IP and trade secrets protection apply irrespective of the nature of data (personal or non-personal). It is likely that (only) GDPR rules should apply to personal data covered by IP rights or trade secrets, as the Data Act is without prejudice to the Union's data protection and privacy framework.

Second**,** personal and non-personal data are increasingly hard to distinguish.[284] It can thus be hard to establish whether the relevant data qualifies as personal or non-personal data, and thus which rules – Article 48 GDPR or Article 27 Data Act - should apply.

Third, while Article 27 Data Act certainly builds on Article 48 GDPR, the two provisions contain nonetheless different rules. In addition, Article 48 GDPR (still) raises serious interpretation issues, notably as regards its 'without prejudice' clause (see figure). The introduction of Article 27 Data Act may thus add to the already existing confusion for providers of data processing services as to how they are expected to deal with foreign governments' requests, in particular when it comes to assessing the rule of law guarantees offered by the relevant third country. In the absence of a mutual legal assistance

[284] Inge Graef, Raphael Gellert, and Martin Husovec, , 'Towards a Holistic Regulatory Approach for the European Data Economy: Why the Illusive Notion of Non-Personal Data is Counterproductive to Data Innovation' (2018) TILEC Discussion Paper No. 2018-029 <https://ssrn.com/abstract=3256189> accessed 10 October 2022.

treaty and mandatory verification of rule of law guarantees by relevant authorities, the Data Act may turn providers of data processing services into regulators.

Eventually, compliance with the new rules may be challenging for providers of data processing services. It may thus be worth considering the application of a single regime in case of international access or transfers of data upon request by foreign governments, irrespective of the nature of the data (personal or non-personal).

## 13. Chapter IX of the Data Act – Data-specific enforcement – Charlotte Ducuing[285] and Aliki Benmayor[286]

In terms of enforcement, the Data Act proposal builds upon the pattern already visible with the DGA and creates another layer of (same or other) enforcement authorities. It establishes 'dispute settlement bodies' ('DSBs') in charge of settling disputes between data holders and data recipients on FRAND terms as per Chapter III.[287] Like the DGA,[288] 'competent authorities' shall also be established (or established bodies shall be granted the associated jurisdiction) to enforce, seemingly,[289] the whole of the substantive provisions of the Data Act proposal, either on their own initiative or following a complaint.[290] Additionally, the Data Act proposal grants supplementary competences to the 'European Data Innovation Board' (EDIB)[291] created by the DGA.[292] While 'competent authorities' are mainly competent to handle complaints, conduct investigations and impose remedies, including financial penalties, the EDIB is entrusted with an advisory and facilitating role. Relatedly, competent authorities shall be independent from market operators and concerned individuals while the EDIB consists of a gathering of a broad range of stakeholders, including private bodies.

The Data Act proposal provides that competent authorities shall cooperate and exchange information,[293] while it will be for Member States to organise such interactions and/or to centralise competences.[294] Additionally, competent authorities shall also cooperate with data protection

[285] Doctoral researcher at Centre for IT & IP Law (CiTiP), KU Leuven, Belgium.

[286] Researcher at Centre for IT & IP Law (CiTiP), KU Leuven, Belgium.

[287] 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 (Data Act proposal), art 10.

[288] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 [2022] OJ L 152/1 (DGA), arts 13 and 23.

[289] In this respect, the Max Planck Institute rightly points to the question whether member States will be allowed to differentiate, for example penalties, depending on the rights and obligations laid down in the Data Act, 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 No. 22-05, para 242 <https://pure.mpg.de/rest/items/item_3388757_4/component/file_3395639/content> accessed 7 October 2022.

[290] Data Act proposal, art 31.

[291] Data Act proposal, art 27(3).

[292] DGA, art 29.

[293] Data Act proposal, art 31(1); see also DGA, art 13(3).

[294] For example, the French *Conseil d'Etat* made several proposals for the government to centralise AI-related enforcement with the French DPA (CNIL), while it could substantively relate to areas as diverse as electronic communications, (cyber)security and sectoral regulations, see *Conseil d'Etat, Intelligence artificielle et action publique : construire la confiance, servir la performance* (Council of State, Artificial Intelligence and public action: the building of trust and performance delivery), 31.3.2022 (https://www.conseil-etat.fr/en/news/turning-to-artificial-intelligence-for-better-public-service. The study is however available only in French). In the field of network industries, France also centralised the, once scattered, enforcement of transport mode-specific legal frameworks with the 'Autorité de Regulation des Transports' (transport regulatory authority), https://www.autorite-transports.fr/ accessed October 10 2022.

authorities established by data protection law,[295] which are responsible for enforcing personal data protection-related provisions of the Data Act.[296] In such cases, 'relevant member States shall designate a coordinating competent authority'. Cooperating authorities – including DPAs - shall then 'ensure the consistent application of the [Data Act]'.[297]

This section analyses the enforcement mechanisms laid down by the Data Act, focusing on the cooperation between the relevant independent administrative enforcement authorities ('IAEA'). The increasing need for cooperation between such authorities with respect to 'data' is not new. However, the first sub-section argues that with the Data Act following the DGA, a novelty lies in the creation of data-specific legislation and ensuing data-specific enforcement authorities. The second sub-section raises the question of whether the required cooperation between enforcement authorities could interfere with the role and independence of DPAs.

This section does not discuss other aspects related to enforcement, such as the establishment and role of DSBs[298] or any cross-border aspects. The relationship with the other legislative proposals currently under discussion, meaning the Digital Services Act[299] and the Digital Markets Act,[300] is also not discussed.

## 13.1. The new era of 'data' legislation and related enforcement

At first glance, the Data Act and the DGA are only yet other examples of legislative frameworks amongst the many that mandate the establishment of dedicated IAEAs. The obligation to cooperate between them and with other relevant authorities is also nothing new. However, we submit that the specificity and novelty of the Data Act and DGA lie in the ambition to create data-specific legislation and ensuing AIEAs.

AEIA are numerous. Most of them are competent for a specific branch of law, such as competition law and personal data protection law,[301] or a specific sector, with the prominent cases of liberalised network industries.[302] For instance, 'national regulatory authorities' (NRAs) are competent with respect to electronic communications law, as per the European Electronic Communications Code

[295] Data Act proposal, art 31(4).

[296] Ibid, art 31(2)(a).

[297] Data Act proposal, art 31(4). Similarly, the DGA mandates authorities relevant for the enforcement of data intermediation – in other words, competent authorities, DPAs, competition authorities, cybersecurity-related authorities and sectoral authorities - to "aim to achieve consistency in the decisions taken in applying [the DGA]", DGA, art 13(3).

[298] However, it is clear that they constitute yet another forum for enforcement and may thus reinforce some of the issues discussed here. Additionally, they come with a risk of further aggravation of the privatisation of adjudication with no well-founded rationale, as elaborated also in Drexl and others (n 290) para 113.

[299] Commission, 'Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC COM/2020/825 final (DSA proposal).

[300] Commission, 'Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act)' COM/2020/842 final (DMA proposal). At the time of writing the European Parliament and the Council have agreed on a text, which has however not yet passed the whole procedure until its entry into force.

[301] Or 'independent supervisory authorities'. The competences of DPAs are laid down in GDPR, art 55. More generally on DPAs, see GDPR, Ch VI. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L 119/1 (GDPR).

[302] For a typology of regulatory authorities, see Hubert Delzangles, 'L'émergence d'un modèle européen d'autorités de régulation' (2011) 692 Revue juridique de l'économie publique, 2.

(EECC).[303] In the case of the Data Act, a first novelty therein lies in the establishment of data-specific authorities, namely authorities entrusted with the enforcement of data-specific legislations. This essentially confirms a phenomenon already visible with the DGA to treat 'data' as a separate regulatory subject matter and a new branch of law.[304]

A second and related novelty is that the substantive rules knowingly borrow concepts from a variety of branches of law, which are brought together in data-specific provisions. For instance, the regulation of data intermediaries under Chapter III of the DGA includes provisions related to security, personal data protection law, competition as well as provisions inspired by the ex ante regulation of liberalised network industries.[305] Additionally, the regulation of 'data' also implies to regulate the interface with other legal frameworks. This is the case with intellectual property rights, trade secrets and personal data protection law, and as particularly visible with the regulation of IoT data (on this, see sec. 15 of this White Paper).[306] Logically, the Data Act does not provide an abstract answer on how to govern the interface with all such legal frameworks. For example, the Data Act refers in several instances to the GDPR,[307] which implies that several AEIAs, including at least a competent authority and a DPA, are likely to be called upon to decide and/or guide companies and individuals on such matters. Subject to future (data space-specific) regulation, interfaces with sectoral legislations are also likely to occur in the application of FRAND terms to different sectors and domains.

Both elements converge in raising the chance that AEIAs will have to cooperate, not only as anticipated by the Data Act and the DGA, respectively. But it is also expectable that other AEIAs be interested in the Data Act, for example, in the field of consumer law, commercial law (that is, the regulation of unfair commercial practices), as well as AEIAs in charge of the enforcement of online platforms.[308]

## 13.2. Interactions between IAEA's: risks for DPAs role and independence

The obligation for authorities to 'aim to achieve consistency' in the Data Act, following the DGA, raises specific questions about the role and independence of DPAs.

There is undoubtedly a principal contradiction between the Data Act, again following the DGA, which generally aims to enhance data sharing and the GDPR, which generally aims to protect individuals concerning the processing of data related to them. DPAs shall, in principle, 'ensure a fair balance

[303] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code [2018] OJ L 321/36 (EECC), Art 5. More generally on NRAs, see EECC, Title II, Ch I.

[304] On the rise of data as a regulatory subject-matter, see Charlotte Ducuing, 'Beyond the Data Flow Paradigm: Governing Data Requires to Look beyond Data' (2020) Technology and Regulation Special Issue: Governing Data as a Resource, 57,59; Thomas Streinz, 'The Evolution of European Data Law (Chapter 29)', in Paul Craig, and Gráinne de Búrca (eds), The Evolution of EU Law (3rd Edn, Oxford University Press, 2021); Charlotte Ducuing, 'The Regulation of "Data": A New Trend in the Legislation of the European Union?' (CITIP Blog, 6 April 2021) < https://www.law.kuleuven.be/citip/blog/the-regulation-of-data-a-new-trend-in-the-legislation-of-the-european-union/>; Charlotte Ducuing, 'An Analysis of IoT Data Regulation under the Data Act Proposal through Property Law Lenses' (2022) CiTiP Working Paper 2022, 15–16 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4225027> accessed 11 October 2022.

[305] Julie Baloup, Emre Bayamlıoğlu, Aliki Benmayor, Charlotte Ducuing, Lidia Dutkiewicz, Teodora Lalova, Yuliya Miadzvetskaya, Bert Peeters, 'White Paper on the Data Governance Act' (2021) CiTiP Working Paper, sec 4 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3872703> accessed 10 October 2022.

[306] Data Act proposal, Ch II.

[307] Ibid, see art 4(5), art 5(6), art 17(2)(d), art 18(5).

[308] In this respect, the Position Statement of the Max Planck Institute interestingly noted an inconsistency with the Digital Markets Act, with respect to the enforcement of the obligations of online gatekeepers under art 5(2)(a) to (c) of the Data Act proposal, between competent authorities - as for the Data Act - and the EC – exclusive enforcer as for the Digital Markets Act, Drexl and others, (n 290) para 92.

between […] privacy and […] the interests requiring free movement of personal data'.[309] The obligations to cooperate and to aim for consistency in the application of the DGA and Data Act could easily tip the balance in favour of the latter. Whether this is a positive or negative development is not only a political question but also a legal one. The 'complete independence' of DPAs, including from *other DPAs* when possibly interfering with their tasks, constitutes a legal principle with Treaty-based legal value, as recognised by the Court of Justice.[310] It cannot be ruled out that the obligation to cooperate and especially seek consistency with other AEIAs entrusted with contradictory objectives could affect the independence of DPAs and the overall mandate they are entrusted with.

Another related risk of the potential blurring of competences arising from the requirement to apply the Data Act proposal consistently, is to equalise the different AEIAs in the face of the law. However, they don't share the same constitutional value. Indeed, DPAs' authority stems directly from primary law, Article 16(2) TFEU[311] and Article 8(3) of the EU Charter on Fundamental Rights (EU Charter).[312] This is justified as their main aim is to safeguard the protection of the data protection right, which is enshrined in EU primary law. The Court has also confirmed that the establishment and role of DPAs represent a constituent element of individuals' protection.[313] Conversely, competent authorities under the Data Act would arguably solely rely on the Treaty's general internal market provision (Article 114 TFEU), which does not justify the potential encroachment over DPA's role.

## 13.3. Conclusions and recommendations

The DGA and the Data Act proposal illustrate the growing interaction between many branches of law with 'data' as a focal point. Additionally, the entrustment of enforcement tasks to 'competent authorities' inevitably results in overlaps between such competent authorities and legacy authorities. This affects both the expertise and swiftness expected from such enforcement mechanisms and therefore raises unpleasant foundational questions such as (i.) whether the appointment of IAEAs is desirable in the first place for the whole of the substantive provisions of the Data Act and (ii.) whether their data-specific focus can be reconciled with the branch of law-specific and the sector-specific focus of legacy authorities. Another possible avenue could simply be to let the judiciary play the role of first-line enforcer in case of disputes, as a by default rule.[314]

---

[309] Case C-518/07 *European Commission v Federal Republic of Germany* [2010] ECR I-01885, paras 24,30.

[310] Consolidated Version of the Treaty on the Functioning of the European Union [2012] OJ C 326/47 (TFEU), art 16 and Case C-210/16 *ULD v Wirtschaftsakademie* [2018] ECLI:EU:C:2018:388, paras 68-73. Charlotte Ducuing, Jessica Schroers, and Els Kindt, 'The Wirtschaftsakademie Fan Page Decision: A Landmark on Joint Controllership – A Challenge for Supervisory Authorities Competences' (2018) 4(4) European Data Protection Law Review 547

[311] Article 16(2) TFEU reads: '*The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities*'.

[312] Article 8(3) of the EU charter reads: 'Compliance with these rules (i.e., right to data protection rights) shall be subject to control by an independent authority'. Charter of Fundamental Rights of the European Union [2012] OJ C 326/391, art 8(3).

[313] *European Commission v Federal Republic of Germany* (n 310) para 25.

[314] The Max Planck Institute also questions the legitimacy of entrusting administrative authorities to enforce the whole of the Data Act substantive provisions, Drexl and others (n 274) 86–88. They seem to equate 'administrative enforcement' with 'public enforcement' on the one hand, and 'judiciary enforcement' with 'private law enforcement' on the other, therefore contrasting the two. This division seems simplistic, while every member State has its own legal enforcement traditions. See also similarly Matthias Leistner and Lucie Antoine, 'Attention, Here Comes the EU Data Act! A Critical in-Depth Analysis of the Commission's 2022 Proposal' (2022) JIPITEC 13, no. 3, para. 20. This being, we support the finding that administrative

Should IAEAs be established, the delineation of their respective roles and competences shall be carefully designed, as it will affect their enforcement practices. In doing so, lessons can be drawn from earlier experiences. In such case, it is advisable that the Data Act further regulates the conditions in which the cooperation between the respective IAEAs shall take place. This recommendation is reinforced by the conclusions of the Advocate General of 20 September 2022 in the case *Meta Platforms v Bundeskartellamt*[315] who invites the EU legislature to adopt 'clear rules on cooperation mechanisms' between competition authorities and DPAs when interpreting the provisions of the GDPR.[316] Stakeholders also need to be consulted with real-life data scenarios that would allow them to identify and navigate potential enforcement issues.

Finally, emphasis should be placed on ensuring that the role of DPAs is not diluted from their original purpose, safeguarding the right to data protection, as enshrined both under Article 16 (2) TFEU and Article 8 (3) of the EU Charter. The obligation to aim for a consistent application of the Data Act seems particularly problematic and should be deleted.

## 14. Chapter X of the Data Act and the Sui Generis Database Right – Thomas Margoni,[317] Thomas Gils[318] and Eyup Kun[319]

This analysis focuses on Chapter X of the Data Act proposal and how it addresses the Sui Generis Database Right. Chapter X features only one article (Article 35) excluding SGDR protection for certain categories of data, namely IoT data. Some additional references to the SGDR can be found in the Preamble of the Data Act. In this section we briefly trace the development of the SGDR and of its relationship to machine-generated and IoT data and identify some long-lasting unresolved issues. We find that Chapter X represents one of the most interesting legislative developments that this area of law has witnessed in recent years. Nevertheless, some substantial space for improvement is still present.

### 14.1. Background: Data Act & the database sui generis regime

Back in 1996, the then-called European Community published Directive 96/9/EC on the legal protection of databases (the Database Directive). Among other things, the Directive created a new sui generis database right to protect databases if a qualifying substantial investment in the obtaining, verification or presentation of content was made. By offering a remedy against the extraction and re-use of the whole or a substantial part of a protected database's content, the SGDR effectively protects (substantial amounts of) data contained in the database, although it does not extend to the single datum or insubstantial parts. Since its inception, the SGDR has been closely scrutinized by Courts and by the same European Commission through two evaluations.[320] Perhaps one of the most contentious

enforcement is not a by default and should therefore be duly justified, which is not necessarily the case for the whole of the Data Act.

[315] Case C-252/21, *Meta Platforms v Bundeskartellamt*, Opinion of AG Rantos, paras 28-33.

[316] Ibid. para 29.

[317] Research Professor of Intellectual Property Law at the Faculty of Law and Criminology, KU Leuven, and a member of the Board of Directors at the Centre for IT & IP Law (CiTiP).

[318] Researcher at Centre for IT & IP Law (CiTiP), KU Leuven, Belgium.

[319] imec- Doctoral Researcher at Centre for IT & IP Law (CiTiP), KU Leuven, Belgium.

[320] Commission, 'DG Internal Market and Services, First evaluation of Directive 96/9/EC on the legal protection of databases' (2005).

elements that emerged from these diverse examinations was the distinction between investments in creating versus in obtaining data. Whereas the former are generally excluded from protection due to their potential anticompetitive effects, the latter are at the core of the Directive's scope. This distinction between creating and obtaining data, however, is not only often difficult to conceptualize, but it is also problematic to implement.

Taking this and other issues into account, the EC set forth an ambitious plan to review the Database Directive in the context of the Data Act in the 2021 Action Plan on IP.[321] The review's goals included the facilitation of the sharing of, and trading in, machine-generated data and data generated in the context of the Internet of Things. Recognizing or rejecting a property or quasi-property right in data has obvious consequences on the nature and structure of data-sharing transactions. In this brief analysis, we will focus on the provisions that attempt to coordinate the rules on SGDR in the Data Act.

## 14.2. SGDR in the Data Act

Only one provision (Article 35) and two recitals (Rec. 84 and 63) of the Data Act explicitly relate to the SGDR. Article 35 states that in order not to hinder the exercise of the right of users to access and use IoT data (as established in Article 4 Data Act) or to share such data with third parties (Article 5), the SGDR does not apply to databases containing data obtained from or generated using an IoT product or a related service.

Rec. 84 explains that in order to eliminate the risk that holders of data in databases obtained or generated by IoT products claim the SGDR, the Data Act should clarify that the SGDR does not apply to such databases. Following the recital's rationale, this is necessary to avoid hindering the effective exercise of the right of users to access, use or share data.

Another interesting provision is contained in Rec. 63 where it is stated that data holders should exercise the SGDR in a way that does not prevent public sector bodies from obtaining and sharing data in accordance with the Data Act (Business to Government or B2G data sharing). This provision must be read in conjunction with the 'proportionate, limited and predictable framework necessary for the making available of data by data holders' to PSBs and Union institutions in cases of exceptional needs, such as public emergencies, or to maintain their capacity to fulfil specific tasks explicitly provided by law (Rec. 61-62). Under this framework and within the circumstances provided, PSBs or Union institutions can file a request to obtain specific data from a data holder. Data holders cannot decline or demand the modification of such requests except in certain specific cases, like the unavailability of the data or incomplete requests.[322]

<https://ec.europa.eu/info/sites/default/files/evaluation_report_legal_protection_databases_december_2005_en.pdf> accessed 11 October 2022; Commission Staff Working Document, Evaluation of Directive 96/9/EC on the legal protection of databases SWD(2018) 146 final <https://ec.europa.eu/newsroom/dae/redirection/document/51764> accessed 11 October 2022.

[321] Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Making the most of the EU's innovative potential An intellectual property action plan to support the EU's recovery and resilience' COM(2020) 760 final <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52020DC0760> accessed 11 October 2022.

[322] 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 (Data Act proposal), art 18, paras 2-3.

## 14.3. Clarifications, amendments and residual unclarity

Despite the proposal's welcome clarificatory purpose, some uncertainties endure.

First, it seems unclear whether the first part of Article 35 should be understood as a functional limitation of the scope of the exclusion (that is, only when the rights listed in Article 4 and 5 are hindered) or rather as a general introductory statement (meaning that a property right in data will always hinder the exercise of those rights, thus the SGDR is always excluded in relation to IoT data). If the intention is the latter, as Rec. 84 seems to purport, removing the first part of Article 35 and placing it in Rec. 84 could help to eliminate any possible doubt relating to the scope of the exclusion. Second, in its current wording, Article 35 excludes SGDR protection for databases containing data obtained from or generated using a product or a related service. Admittedly, the provision intends to exclude (or better, to confirm the ineligibility of, see Rec. 84) databases consisting of machine-generated data from SGDR. However, the choice of words may be problematic since it has the potential to contrast with the plain language of the Database Directive and Court of Justice of the European Union (CJEU) pronouncements.

Indeed, Article 7 of the Database Directive requires Member States to grant SGDR to the maker of a database if there is a substantial investment in the obtaining, verification, or presentation of the content. One of the elements frequently litigated before the courts is precisely the exact contour of the investments in creating data *versus* the investments in obtaining data and the relationship between the two types of investments. This delineation is especially relevant in the light of the fact that, in many situations, both investments may coexist and it may not be easy to separate them.[323] In this regard, the CJEU had the opportunity to clarify that when determining whether the creator of a database has made a substantial investment in obtaining the database's contents, the resources utilised to create the elements should not be considered.[324] The CJEU based its decision on various recitals of the Directive, citing as decisive the fact that, according to Recitals 9, 10, 12 and 39, the objective of the Database Directive is to promote and protect investments in the development of storage and processing systems, not in data creation.[325] In other words, investments in data creation do not count towards a finding of SGDR. Scholars have overall argued in favour of this type of distinction, since the protection of created data with property or quasi-property rights have strong anti-competitive effect on the free flow of information, including in cases of so called single-source databases.[326] It is interesting to note that the first version of the Directive duly considered this type of anticompetitive effects and had put in place a system of compulsory licences in cases of created data, an option that was eventually abandoned in the approved text of the Directive.[327]

---

[323] Case C-203/02, *British Horseracing Board v. William Hill Organization* [2004] ECR I-10415 (BHB); Case C- 338/02, *Fixtures Marketing v. Svenska Spel* [2004] ECR I-10497 (Svenska Spel).

[324] *BHB* (n 324) para 31; *Svenska Spel* (n 324) para 24.

[325] *BHB* (n 324) paras 30, 32.

[326] P.B Hugenholtz, 'Program schedules, event data and telephone subscriber listings under the Database Directive: the spin-off doctrine in the Netherlands and elsewhere in Europe' (Fordham School of Law 11th Annual Conference on International Intellectual Property Law and Policy, 2003) <https://www.ivir.nl/publicaties/download/spinofffordham.pdf> accessed 11 October 2022.

[327] See Article 8(1) of the proposed version of the Database Directive. Commission, 'Proposal for a Council Directive on the legal protection of databases' COM(92) 24 final — SYN 393, 4 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:51992PC0024>.

As a result of these legislative and interpretative developments, it is now settled law that only investments in the obtaining, not in the creation of data qualify (as seen, for example, in *BHB*[328] and Svenska Spel[329]). Therefore, when the proposed Article 35 puts on the same level "obtained" and "generated" data this may create ambiguities given the semantic closeness of the words creation and generation. An example of this conceptual ambiguity can be found in AG Stix-Hackl Opinion in the BHB case: '"obtaining" within the meaning of Article 7(1) of the Directive does not cover the mere production of data, that is to say, the generation of data'.[330] Accordingly, the use of a textual formulation that puts on a functionally equivalent level 'obtained' and 'generated' data creates confusion as to the scope of the provision here under analysis, in particular whether Article 35 is simply a clarification of the current law or an attempt to amend it. This situation is made even more puzzling in the light of the fact that the creation v. obtaining dichotomy may be particularly difficult to conceptualize when the data is simply observed or recorded from nature or the surrounding environment, as it may often happen with IoT (see Rec. 14&15 Data Act). This is, with no doubt, one of the main uncertainties currently affecting the SGDR (see Data Act Explanatory Memorandum at p. 9), which is certainly intensified by the Data Act's goal of regulating an already borderline category of data, such as machine generated IoT data.

As a preliminary conclusion on this aspect, we suggest that if the goal of Article 35 Data Act is to clarify that IoT data simply do not enjoy SGDR protection, since they (almost?) never did, perhaps a simpler statement that for the purpose of Article 7 Database Directive IoT data as defined in the Data Act are created data and therefore excluded from protection ab origine (and ex tunc) may be preferrable. This may in fact fully qualify as a clarification of the law (a sort of authentic interpretation) given the current existing and acknowledged uncertainty on the creation/obtaining dichotomy. It would also probably avoid issues of temporal applicability raised in the literature.[331]

Third, it may be argued that it is currently not fully clear who are the recipients of Article 35, whether only data users and data holders (including the manufacturer of IoT products and services) or also third parties. In fact, it could easily be contended that a third party who invests substantially to obtain data from either the data holder or the data user (like through the payment of a fee) or to verify or present the data (for example, validate their content, index and present them), may, under current law (pre-Data Act), enjoy SGDR protection. If the goal of Article 35 is to exclude also these third parties from SGDR then it will probably be more difficult to justify this effect on the grounds of a simple clarification of the law. On the other hand, if the current opening of Article 35 is meant to address the issue in the sense that third parties may still qualify for SGDR, then perhaps, in addition to removing the current first part of Article 35 (as suggested above), a new paragraph 2 in Article 35 could state that paragraph 1 is without prejudice to the ability of third parties to enjoy SGDR protection provided that the conditions of Article 7 et seq Database Directive are met. This second option seems preferable, as it would share most of the policy concerns limiting or excluding from protection single source databases.

---

[328] See *BHB* (n 324).

[329] See *Svenska Spel* (n 324).

[330] *BHB* (n 324), Opinion of AG Stix-Hackl <https://curia.europa.eu/juris/document/document.jsf?text=&docid=48761&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=514373#Footnote10>, accessed 11 October 2022.

[331] ECS, Opinion of the European Copyright Society on selected aspects of the proposed Data Act (12 May 2022) <https://europeancopyrightsocietydotorg.files.wordpress.com/2022/05/opinion-of-the-ecs-on-selected-aspects-of-the-data-act-1.pdf> accessed 11 October 2022.

Fourth, regarding the important obligation contained in rec. 63, in order to confirm its full effectiveness, the last sentence of rec. 63 should be moved to and/or reiterated in a dedicated paragraph in Article 35 or 35 bis. Furthermore, to fulfil the ambitious and key objective of favouring B2G data sharing, it should be considered to extend the scope of such provision to address the SGDR, other types of intellectual property regimes, deontological duties, technical circumstances, among others. This is currently explicitly left out of the scope of the proposal. The explanatory memorandum mentions on p.5: 'This proposal does not affect existing rules in the areas of intellectual property (except the application of the sui generis right of the Database Directive) (…)' This is understandable as introducing new exceptions to or amending the scope of protection of IP rights is often a highly political matter. On the other hand, interfering with the SGDR may be less of an issue due to its sui generis character and specific objective of protecting a substantial investment. However, this is not explicitly acknowledged by the proposal and begs us the question of why other types of intellectual property regimes, deontological duties or technical circumstances are not addressed in rec. 63. After all, many other considerations may be invoked by data holders in order to avoid having to share data or to feign data unavailability. For instance, the requested data may only be available in a certain data structure or format, which may be subject to patent protection.[332] In such hypothesis, the requesting PSB or Union institution will, in principle, have to obtain a patent licence because neither the existing exceptions to patent protection (see, for example, Article 27 UPC Agreement)[333] nor the existing possibilities to grant a compulsory licence cover this type of situation. Similarly, data holders may be bound by deontological duties (like professional secrecy) or confidentiality obligations (such as non-disclosure agreement (NDA)), whereby it is unlikely that existing exceptions to professional secrecy obligations, existing NDAs or the special regulations on trade secrets allow for the B2G data sharing envisaged by the Data Act.[334] Finally, data holders may make data available in an encrypted or proprietary data format which may render the data inaccessible to PSBs or Union Institutions. This latter consideration may be solved by clarifying the scope of the general obligation to make data available under Article 14 §1 and/or 18 §1 (for example, does that entail decrypting data and/or providing data in commonly used data format?).

Fifth, the abovementioned remarks relating to the possible restrictive impact of intellectual property regimes, deontological or confidentiality duties, trade secret regulation and technical circumstances on B2G data sharing should also be considered mutatis mutandis in the context of B2C or B2B data sharing (Chapter II and III Data Act). For instance, suppose a data holder would have to make IoT data available to a third party under Article 5 Data Act and said IoT data only exists in a proprietary, patented data format. Under the current regime and with the lack of applicable exceptions or compulsory licences, the third party should obtain a patent licence in the absence of which a patent infringement

[332] EPO Guidelines for examination, G-II-3.6.3: Data retrieval, formats and structures <https://www.epo.org/law-practice/legal-texts/html/guidelines/e/g_ii_3_6_3.htm> accessed 13 September 2022.

[333] Council, Agreement on a Unified Patent Court [2013] OJ C 175/1, art 27, 1–40.

[334] In this context, it is worth mentioning that Art. 19.2 indeed refers to the disclosure of trade secrets. However, based on the reference in Art. 8 to Directive (EU) 2016/943 (i.e. the Trade Secrets Directive), it can be presumed that the Data Act understands trade secrets as defined in Art. 2 Trade Secret Directive. Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure [2016] OJ L 157/1 (Trade Secrets Directive). Said definition does not necessarily cover all data subject to professional secrecy or confidentiality obligations. In other words, when certain information falls under the definition of trade secret as put forth by the Trade Secrets Directive, it is covered by art. 19 Data Act. Oppositely if such information does not fall under said definition, then it is also not covered by art. 19 Data Act, while it could nonetheless fall under certain professional secrecy or confidentiality obligations.

could arise. However, a data holder is not obliged to grant such licence, which could hinder the envisaged data sharing.

## 14.4. Conclusions

For the first time since its inception in 1996 the SGDR has been object of a legislative intervention intended to demarcate its scope. Whether this is by a clarification or (also) by a change in the law remains to be seen in the light of the above reflections. In any event, the spirit of Article 35 is a welcome intervention from the perspective of favouring competition, users' choice and data sharing. Arguably, the provision does not live up to the expectations of those awaiting a more substantial review of the Database Directive. However, perhaps more news on this front will come in a future amending directive.

# 15. The Data Act and the 2016 Trade Secrets Directive – Ella De Noyette[335] and Thomas Margoni[336]

This chapter focuses on the coordination of the data access rights provided by the Data Act proposal on the one hand and the protection of trade secrets on the other. With references throughout the proposed Regulation,[337] trade secrets were far from forgotten in the drafting of the Data Act. However, as it may be expected from such a complex and innovative piece of legislation, several questions remain unanswered. This chapter will first explore the general interrelationship of the Data Act and the 2016 Trade Secret Directive, and the challenges of uniting these two approaches. It will further elaborate on more specific issues of concern, focusing on Article 8(6) Data Act.

## 15.1. A shared data sharing objective

The 2016 Trade Secret Directive[338] (TSD) harmonised the rules against the unlawful acquisition, disclosure and use of Trade Secrets in order to enhance competitiveness, innovation and investments in the knowledge economy. As argued in the same TSD, trade secrets have an important role in protecting and facilitating the exchange of knowledge between businesses and research institutions within and across the borders of the internal market (as seen in Rec. 3 TSD). A comparable - and arguably complementary – knowledge-sharing ambition can be found in the recent Data Act proposal, for instance, in the provisions on making data generated using IoT products available to their user (Article 4 Data Act) and to designated third parties (Article 5 Data Act), as well as in relation to rules on B2B and B2G data sharing.

## 15.2. Two different approaches

[335] PhD researcher at Centre for methodology of law and Centre for IT & IP Law (CiTiP), KU Leuven Kulak, Belgium.

[336] Research Professor of Intellectual Property Law at the Faculty of Law and Criminology, KU Leuven, and a member of the Board of Directors at the Centre for IT & IP Law (CiTiP).

[337] 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 (Data Act proposal), arts 4, 5, 8, 17 and 19; recs 28, 66 and 77.

[338] Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure [2016] OJ L 157/1 (Trade Secrets Directive).

In pursuing the ambitious objective of stimulating data sharing, the Data Act proposal aptly incorporates references to trade secret protection. This is arguably done to coordinate certain regulatory overlaps but also to address the potential clashes that may originate in what could be termed as different – and in certain cases even opposite – approaches to data sharing: the prohibition of certain uses and disclosures on the one hand, and the obligation to provide access and share certain data on the other.

It goes without saying that the object of these prohibitions and obligations may well be the very same piece of data and/or information. Indeed, the definitions of 'data' and 'trade secret' share common ground. Just as any information can be protected as a trade secret if the information is secret, has commercial value because it is secret and reasonable steps have been taken to keep it secret (Article 2(1) TSD), any information can be considered as data if digitally represented (Article 2(1) Data Act).[339]

In any event, the current relevance of trade secret protection for data should be properly contextualised. As shown in a recent empirical investigation, to this day, businesses often do not consider trade secrets as an effective protection mechanism for (shared) confidential and commercially valuable data due to several factors, such as the lack of awareness and knowhow of firms and the general legal uncertainty with regards to trade secret protection and enforcement.[340]

## 15.3. Raw data and inferred information

An important element of discontinuity in the scope of the TSD and of the Data Act is nevertheless represented by so called 'inferred information' (Rec. 14 Data Act), meaning the information derived from data representing the digitalisation of user actions and events. Whereas the latter data is at the core of the scope of the Data Act, information inferred therefrom (where lawfully held) is excluded (Rec. 14). The distinction is logically sound. It seems plausible, in fact, that this derived information, much more than the original 'raw data', has the potential for representing commercially valuable and possibly secret knowledge which, if the requirements are present, will be eligible as TS.[341]

This conclusion could perhaps find additional support later in the preamble, where Recital 17 Data Act offers a parallel exclusion for data resulting from software processes that calculate derivative data

[339] On the definition of 'data', see Julie Baloup, Emre Bayamlıoğlu, Aliki Benmayor, Charlotte Ducuing, Lidia Dutkiewicz, Teodora Lalova, Yuliya Miadzvetskaya, Bert Peeters, 'White Paper on the Data Governance Act' (2021) CiTiP Working Paper, 9-10 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3872703> accessed 10 October 2022. On the possible overlap with the definition of a 'trade secret', see Commission, European Innovation Council and SMEs Executive Agency, Alfred Radauer, Martin A. Bader, Tanya Aplin, Nicola Searle, Reinhard Altenburger, Ute Konopka, Christine Bachner, 'Study on the legal protection of trade secrets in the context of the data economy: final report', Publications Office of the European Union (2022) <https://data.europa.eu/doi/10.2826/021443> and the references made in fn 122 (hereinafter 'Study on TS in the data economy').

[340] Study on TS in the data economy (n 340) 62-74.

[341] Drexl indeed confirms the lower potential of 'raw data', especially when it concerns 'individual (raw) data', by stating that *'only part of the data that a single connected device generates will be capable of being considered a trade secret. In particular, where the data produced by a connected device is very limited and no particular secrecy interest exist, neither on the part of the manufacturer nor of the customer, such as in the case of a smart meter measuring the consumption of energy, such data will most likely not be protected as a trade secret'* (Josef Drexl, 'Data Access and Control in the Era of Connected Devices (Study on Behalf of the European Consumer Organisation BEUC, BEUC, 2018) 94). This is confirmed in the Study on TS in the data economy, (n 319)78-80. Because of the limitation of the Data Act to 'raw data', the authors of the Study conclude the Data Act and TSD '*should not clash'* (page 89). However, Leistner & Antoine rather emphasize that it is possible, and even state this will often be the case: *'individual-level datasets, consisting of comprehensive use data from one user of an IoT device will often have to be regarded as secret'* (Matthias Leistner and Lucie Antoine, 'IPR and the use of open data and data sharing initiatives by public and private actors' (European Union, 2022) 86-87).

since 'such software process may be subject to intellectual property rights'. Questions remain about the intended difference in scope (if any) between derivative data and inferred information. Moreover, it is unclear whether the drafters intended to (also) refer to TS when mentioning IP, given that in legal theory TS is often excluded from the intellectual property field properly construed due to the absence of exclusive rights – an exclusion not necessary adopted in the practice.[342]

## 15.4. Ex post and ex ante approches

The Data Act regulates business-to-consumer, to businesses and to government data sharing while also introducing special rules when these data constitute a trade secret. However, as pointed out by the Max Planck Institute in its position statement (hereinafter MPI statement), whether information qualifies as a trade secret is commonly confirmed ex post, usually before a court. [343] Conversely, the Data Act seems to introduce a sort of ex ante phase where data holders, users and third parties bear specific obligations when the data to be shared may qualify as a trade secret, something that will arguably be left to the determination of the involved parties. Naturally, the fact that different parties usually retain different degrees of bargaining power, combined with the fact that one party (usually the data holder) already exerts control over the data sought by the user, may very well influence the conditions – including the acceptance of a piece of information as TS – that the latter is willing to accept.

Whereas it seems reasonable and even necessary to introduce special rules that regulate a special situation (that is, when data is TS), the reported lack of guidance on who will establish whether a certain piece of data is TS and how this should be done, may lead to uncertain developments. In other words, considering the degree of (real or perceived)[344] vagueness intrinsic in the definition of trade secrets, a data holder may have strong incentives to claim that the data, object of an access or sharing request, is a trade secret and accordingly restrict or even exclude such data from the access and sharing obligations set forth in Articles 4 and 5.[345] It would be arguably cumbersome for users and third parties to counter this type of claims.

## 15.5. Articles 4(3) and 5(8) Data Act: Loopholes beyond the ex ante approach?

The depicted situation may not be particularly problematic in the case of Article 4(3) Data Act (as pointed out by the MPI statement).[346] Article 4(3) Data Act stipulates that when users exercise their right to access and use IoT data, trade secrets should only be disclosed provided that all specific necessary measures are taken to preserve the confidentiality of trade secrets, in particular with respect to third parties. Therefore, users seldom find themselves in a situation compelling them to

[342] TS are generally considered as quasi-IP, see, for example, Thommaso Fia, 'Resisting IP Overexpansion: The Case of Trade Secret Protection of Non-Personal Data' (2022) 53 International Review of Intellectual Property and Competition Law, 924; Nari Lee, Hedging (into) Property? – Invisible Trade Secrets and International Trade in Goods in Jonathan Griffiths and Tuomas Mylly (eds.), Global Intellectual Property and New Constitutionalism: Hedging Exclusive Rights (Oxford University, 2021) 106-128.

[343] 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 No. 22-05, 101, para 280 <https://pure.mpg.de/rest/items/item_3388757_4/component/file_3395639/content> accessed 7 October 2022.

[344] Study on TS in the data economy (n 340) 75-81.

[345] Ibid, 89-90.

[346] Drexl and others (n 344) 101, paras 281-282.

counter a possibly unsubstantiated TS claim. At least as long as they are willing to accept a confidentiality request. Nevertheless, it should be noted that this situation would introduce an additional duty of care and consequent liability profile on users who are now aggravated by a confidentiality obligation in relation to IoT data that represent their own behaviour.

The case of Article 5(8), however, may be different. The article stipulates that trade secrets shall only be disclosed to third parties to the extent that they are strictly necessary to fulfil the purpose agreed between the user and the third party and that all specific necessary measures agreed between the data holder and the third party are taken by the third party to preserve the confidentiality of the trade secret. Consequently, it seems at least plausible that Article 5(8) may be used to artificially block or dilute data sharing requests, including legitimate ones, when the requested data is identifiable with the claimed TS.

At present time, it seems difficult to assess the potential of this loophole in the data sharing obligations to frustrate the overall goals of the Data Act. Certainly, it is crucial at this stage of the legislative process to find a proportionate balance between data sharing obligations and the legitimate protection of trade secrets. Perhaps, putting at the centre of this effort the normative goals of both legislative interventions – that is, favouring the sharing of data in a fair and trusted environment to enhance innovation and competitiveness – should be the guiding driver of future amendments. Confidentiality obligations, much more than the possibility to avoid sharing duties tout court – especially when data holders may have strong and unhindered incentives to overclaim trade secrets over co-generated data – seem to appropriately capture this balance.

## 15.6. Article 8(6) Data Act: lost in interpretation?

Article 8(6) stipulates that, unless otherwise provided by Union law, including Article 6 of this Regulation, or by national legislation implementing Union law, an obligation to make data available to a data recipient shall not oblige the disclosure of trade secrets within the meaning of the TSD. At first sight, it seems self-evident that there is no general obligation (arguably for the data holder) to disclose trade secrets. It would honestly be difficult to argue anything different, especially in the light of the provisions set forth in Articles 4(3) and 5(8) on the relationship between the rights of users to access, use and share data with third parties on the one hand and the protection of trade secrets on the other.

At second glance, however, Article 8(6) is of more difficult exegesis. As pointed out in other comments and studies, there appear to be several textual incongruences in this article, including missing or inaccurate references.[347] This seems unusual for an EU official document, even for a draft. In fact, a textually consistent reading may be present.

## 15.7. The interpretation of 'disclosure'

It is plausible that the main cause of incongruity with the current wording of Article 8(6) and the other provisions of the Data Act rests on the specific conditions under which a TS may be disclosed and the effect of these different types of disclosures.

Accordingly, within the aforementioned Articles 4(3) and 5(8) 'disclosure' may only happen under confidentiality conditions. This confidentiality requirement seeks to preserve the trade secret. This

[347] Ibid, 102, paras 283-284; Leistner and Antoine (n 342) 102-103.

way, these mandatory and confidential disclosures strike a specific balance between the Data Act approach (sharing obligations) and the TSD approach (protection of TS).

On the contrary, Article 8(6), in (re)affirming a general prohibition of TS disclosure, uses the word 'disclosure' in absence of any confidentiality condition, therefore arguably referring to the unlawful disclosures regulated in the TSD and not to the confidential (and necessarily lawful) disclosure mandated in Articles 4(3) and 5(8). Otherwise, the reference in Article 8(6) to the TSD ('within the meaning of Directive (EU) 2016/943'), absent in Articles 4(3) and 5(8), would be redundant. This reconstruction would also help explain why, differently from Article 6, Articles 4(3) and 5(8) are not referenced in Article 8(6): they refer to different situations and (confusingly) to a different category of disclosures, namely confidential disclosures.

## 15.8. The reference to Article 6 Data Act: Textual or policy concerns?

Regarding the reference contained in Article 8(6) to Article 6, which has been object of criticism due to its ambiguous positioning, one might wonder whether it was intended to be specific to Article 6(2)(c). In that case, the sense of the provision would be that when a third party receives data at the request of a user and said third party makes the data available to another third party (as this is necessary to provide the service requested by the user), this 'second line' third party is allowed to disclose – in the sense of Article 8(6), that is, with no confidentiality obligations – the trade secrets eventually present in the data. From a purely textual analysis, this interpretation would be consistent and would solve some of the alleged inaccuracies.

Nonetheless, the interpretation would also create an inconsistent situation where the same data could be freely used and disclosed by 'second line' third parties (Article 6(2)(c)), while users and 'first line' third parties designated by users, namely the main beneficiaries of the Data Act, would be systematically bound by confidentiality obligations (Article 4(3) and 5(8)). In other words, the balance between the Data Act approach and the TS approach is already seen in Articles 4(3) and 5(8). In the case of Articles 8(6) and 6(2)(c), it shifts decidedly in favour of the Data Act and against the preservation of TS. This seems an odd conclusion, which may very well weigh against the desirability of the proposed reading and contextually support the view that Article 8(6) is simply poorly written and should be either significantly clarified (as suggested by Leistner & Antoine and Radauer and others)[348] or deleted altogether (as suggested by the MPI statement).[349]

Nevertheless, it should be noted that the fact that a lawful disclosure can happen in absence of a confidentiality obligation between the first and the second line third party within the narrow boundaries of Article 6(2)(c), does not imply that a confidentiality requirement is preempted. In fact, it seems logical (and probably necessary) that the initial disclosure will have to be based on Articles 4(3) and/or 5(8), therefore carrying an ex lege confidentiality obligation for the first line third party. Since this confidentiality obligation required by law must be agreed upon and implemented by the relevant parties (for example, contractually), as long as the agreement embedding confidentiality is adequately drafted, it may very well oblige to confidentiality subsequent disclosures that the first line third party may be required to execute under Article 6(2)(c). In this case, a confidentiality obligation, arguably saving secrecy, will still be required. The only difference is that the legal basis is not statutory,

[348] Leistner and Antoine (n 342) 102-103; Study on TS in the data economy (n 340) 91-92.
[349] Drexl and others (n 344), 102, para 284.

but instead the contract or agreement binding the first line third party to the original data holder. This effect is not only textually consistent but also seems a logical corollary of Article 4(3)(b) and (c) TSD.

If this were the intended meaning of the provisions under analysis, then the overall relationship between TS and data sharing obligations would look as follows. The general rule established in Article 3(2) TSD – and arguably reported for coordination in Article 8(6) Data Act – authorises the disclosure of a trade secret to the extent that it is required or allowed by Union or implementing national law.[350] Articles 4(3), 5(8) and 6(2)(c) Data Act are specific instances of this general principle. The confidentiality conditions therein established follow a decreasing gradient of imperativeness: confidentiality is a requirement under 4(3) and 5(8), whereas in the more remote situation of 6(2)(c) it is simply a possibility left to the discretion (and awareness) of interested market players to be grasped. A contestable policy choice, but a choice, nonetheless. Should this be the legislator's actual intention or a desirable solution, the whole section would need to be better structured and coordinated with the TSD.

## 15.9. B2G sharing of data qualifying as trade secrets

Article 14(1) Data Act obliges the data holder to share data with public authorities at their request when there is an exceptional need to use this data. The rest of the Chapter V provisions further elaborate on this obligation with Articles 17 and 19 referring to the consequences for trade secret protection, among other things.[351] First, Article 17(2)(c) prescribes that a request should respect the legitimate aims of the data holder, considering the protection of trade secrets. It does not clarify how this should be done. However, we may presume that this includes, among others, a prohibition to use the data to develop a product that competes with the product from which the accessed data originate or share the data with another third party for that purpose (thus mirroring Article 6(2)(e)). Second, Article 19(2) requires confidentiality measures in case of disclosure of a(n alleged) trade secret. In addition, the request can only be made if the trade secrets are strictly necessary to achieve the purpose of the request. It is not clear why in this case reference is made to 'alleged' trade secrets, while this is not the case for B2C and B2B disclosure, since the same issue of 'alleged' trade secrets is present, see previous section on the ex ante and ex post approach. Moreover, the strict necessity requirement seems to imply there is a different, probably higher, threshold than the 'exceptional need'.[352]

## 15.10. Some additional areas of clarification

First, Articles 4(3) and 5(8) require data recipients to take all 'specific necessary measures' to preserve the confidentiality of trade secrets. Article 19 mentions 'appropriate measures'. It is unclear whether there is a difference between the two standards, or if these requirements go further than, or are equal to, the 'reasonable steps' required by the TSD for information to be a trade secret.[353] For this reason,

[350] However, if this general rule is already established in Art. 3(2) Data Act, then this should suffice (Study on TS in the data economy, n 340, 91-92). 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 (Data Act proposal).

[351] On Chapter V in general, see Antoine Petel, 'Chapter 5 of the Data Act – What is the european concept of "B2G data sharing" in the Data Act proposal?' (*CiTiP Blog*, 21 June 2022) < https://www.law.kuleuven.be/citip/blog/chapter-5-of-the-data-act-what-is-the-european-concept-of-b2g-data-sharing-in-the-data-act-proposal/>.

[352] Study on TS in the data economy (n 340) 91.

[353] Ibid.

it would be preferred if the Data Act clarified whether and how these thresholds are different or alternatively converged towards a common standard.

Second, it is remarkable how the Trade Secrets Directive pays enormous attention to the procedural guarantees for trade secret protection. This attention lacks in the Data Act: should the data holder designate a trade secret as such, and if so, how? What about disputes on this designated status? Article 10 Data Act addressing aspects of 'dispute settlement' omits any reference to these procedural questions, which seems a missed opportunity to enhance legal certainty and favour standardisation, trust and awareness in the field of TS and data sharing obligations.

## 15.11. Conclusions

Whereas both the Data Act and the TSD share the objective to facilitate the exchange of information, the approaches that they follow diverge, sometimes significantly. The Data Act rightly focuses on the relationship with the TSD, providing specific instances where TS may be lawfully disclosed. This policy choice seems understandable and proportionate to the extent that the disclosures are backed by confidentiality obligations. Arguably, this approach will create incentive for IoT manufacturers to code the collection of data in a way that does not reveal any eventual TS and possibly employ to this end the 'safe harbour' of inferred information. Perhaps, this design principle might well represent the most effective balance between the two approaches.

# 16. Use case: Medical devices – Elisabetta Biasin[354]

## 16.1. Introduction

Since at least 2018, the EU policymaker has highlighted the potential of data to be a 'key enabler for digital transformation in health and care'.[355] As the European Commission put it, data-enabled decisions would 'make it possible to tailor the right therapeutic strategy to the needs of the right person at the right time, and/or to determine the predisposition to disease and/or to deliver timely and targeted prevention'.[356] Data is deemed essential to unlock the potential of personalised medicine,[357] as it 'can increase the well-being of million of citizens and change the way health and care services are delivered, including […] accelerated development of medicines and medical devices'.[358]

[354] Doctoral researcher at Centre for IT & IP Law (CiTiP), KU Leuven, Belgium.

[355] Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions "Towards a common European data space" COM(2018) 232 final (Towards a common European data space), 3.

[356] Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A European Strategy for Data' COM (2020) 66 final (European Strategy for Data), 2.

[357] See Commission, Towards a common European data space, 3. On the notion of personalised medicine, see Griet Verhenneman G, 'The Patient's Right to Privacy and Autonomy against a Changing Healthcare Model' (DPhil thesis, KU Leuven Faculteit Rechtsgeleerdheid 2020).

[358] See Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Empty on enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society' COM(2018) 233 (Communication on digital transformation of health and care), 4.

In the last months, the European legislator released a set of legislative proposals on data sharing, some of which have been general and others specific to healthcare.[359] This chapter aims to illustrate the role and possible issues of the Data Act proposal as applied to the healthcare sector from the perspective of medical devices. The first section introduces the relevance of the Data Act proposal to medical devices. A second section complements this part and includes critical remarks about some definitions of the Data Act proposal for medical devices.[360] The third section contains insights concerning the interplay between the Data Act proposal and other legislative acts (notably, data and cybersecurity law). The conclusion resumes the findings and offers policy recommendations.

## 16.2. The Data Act proposal and medical devices

As the Commission underlined,[361] data may support the accelerated development of medical devices. Moreover, when it comes to AI-based medical devices, data may help diagnose diseases[362] or support clinicians' decision-making.[363] Recent applications imply the creation of 'Digital Patients or Twins', which may support surgeons in their training or planning of their medical interventions.[364] As another example, 'real-world' data may be processed by medical devices to help monitor post-market safety and adverse events and thus support agencies in their regulatory decisions.[365]

The Data Act is designed to constitute a horizontal proposal envisaging basic rules for all sectors for the use of data. The proposal leaves room for vertical legislation to set more detailed rules for achieving sector-specific regulatory objectives. This is the case of the healthcare sector. As the Data Act puts it, the proposal aims to cover physical products that obtain, generate, or collect data ('IoT products'). Recital 14 of the proposal clarifies that 'medical and health devices' shall be considered within these products. As such, the Data Act is expected to apply to medical and health devices.

Medical devices are products regulated by specific legislation in the EU, the Medical Device Regulation (MDR)[366] or the In-Vitro Medical Device Regulation (IVDR)[367]. There exist several types of medical

[359] These include not only the Data Act proposal, but also the European Health Data Space proposal, and the Data Governance Act. 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 (Data Act proposal); Commission, 'Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space' COM/2022/197 final (EHDS); Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 [2022] OJ L 152/1 (DGA).

[360] For reasons of space, the analysis cannot be comprehensive of the whole data act proposal definitions applied to medical devices, the focus is applied to 'data holders' and 'users'.

[361] See Commission, Towards a common European data space, 3. On the notion of personalised medicine, see Griet Verhenneman G, 'The Patient's Right to Privacy and Autonomy against a Changing Healthcare Model' (DPhil thesis, KU Leuven Faculteit Rechtsgeleerdheid 2020).

[362] See, for example, Yogesh Kumar and others, 'Artificial intelligence in disease diagnosis: a systematic literature review, synthesizing framework and future research agenda' (2022) Journal of ambient intelligence and humanized computing 1.

[363] Ibid.

[364] See Hanad Ahmed and Laurence Devoto, 'The Potential of a Digital Twin in Surgery' (2020) 28(4) Surgical Innovation.

[365] See FDA, 'Real-World Evidence' (*FDA, 8 September* 2022) <https://www.fda.gov/science-research/science-and-research-special-topics/real-world-evidence> accessed 9 September 2022; see also International Coalition of Medicines Regulatory Authorities (ICMRA), 'ICMRA statement on international collaboration to enable real-world evidence (RWE) for regulatory decision-making' (2022) < https://www.icmra.info/drupal/sites/default/files/2022-07/icmra_statement_on_rwe.pdf> accessed 9 September 2022.

[366] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC [2017] OJ L117/1 (MDR).

[367] Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU [2017] OJ L117/176 (IVDR).

devices. They are classified based on their risk to patients and end-users. Medical devices may be products or services used by healthcare providers (for example, magnetic resonance imaging (MRI) scanners and X-ray scanners) but also directly by patients (like pacemakers and insulin pumps). Medical devices may also consist of software (including Computer-Aided Detection (CAD) systems, and pregnancy apps).

## 16.3. Applying the Definitions of the Data Act proposal to the Medical Devices' Stakeholders

Who is the data holder? –The Data Act proposal means the data holder as the

> 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.[368] .

In the medical device data sharing scenario, several actors could be involved, including medical device manufacturers, healthcare providers, patients, and healthcare research entities. A medical device manufacturer could be a data holder towards a healthcare provider or the patient (which, in this case, could be users).[369]

There could be some unclarities, however, as to whether healthcare providers could be considered data holders concerning non-personal data. By reading Article 2(6), one might find the second part ('*or*, in case of non-personal data … make available certain data') of the definition quite unclear.[370] What does 'through control of the technical design of the product and related services' mean?

To understand whether a healthcare provider may be a data holder for non-personal data, one should ask: does a healthcare provider has control of the technical design of a medical device put on the market by the manufacturer and related services? The answer seems not to be simple. Difficulty a healthcare provider has control of the technical design of a medical device unless the healthcare provider modifies the intended purpose of the medical device and becomes a manufacturer on its own.[371] It is also difficult to interpret 'and related services'. Suppose one interprets 'related services' as the healthcare services provided to the patient via the healthcare provider. In that case, it remains unclear whether 'and' in the sentence serves a conjunctive or disjunctive function. In other words, it remains unclear if the healthcare provider must have control of the product and the related service conjunctively or whether it is sufficient one of them. In conclusion, the definition of data holder

[368] Data Act proposal, art 2(6)

[369] For broader remarks on the notion of 'user', see sec 16.4.

[370] See also EDPB-EDPS, 'EDPB-EDPS Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)' (2022), 11: 'the definition of "data holder" should be further clarified'.

[371] See MDR, art 16.

requires further clarification.[372] This would be relevant for the Data Act proposal and the EHDS proposal, where a similar phrasing is used.[373]

The (expanded) notion of user – Article 2(6) of the proposal defines the user as 'the natural or legal person that owns, rents or leases a product or receives a service'. For the medical device scenario, that could translate into the following.

> Examples: Patients could be data users towards healthcare providers – because they receive a healthcare service. Healthcare providers could be users towards medical device manufacturers – if they own certain medical devices of a given manufacturer. Third entities could be data users, such as healthcare research facilities towards the healthcare provider, which could be the data holder.

As discussed in sec. 3 of this White Paper (in the matter of data portability), the Data Act proposal considers the role of users for natural and legal persons.[374] What is worth noting in a medical device use case is how this expansion of scope may entail new situations from an ethical or regulatory perspective:

> Example (legal persons): the medical device data are accessed by a user. The data are interpreted by a third-party device software that is not subjected to regulatory scrutiny under MDR.[375] The software provides inaccurate information to the patient about their disease.
>
> Example (natural persons): the patient (user) receives direct access to data revealing the exit of a test.[376] The healthcare professional is not involved in the process or is not placed in the position to explain the results to the patient.

The first example shows how there could be new issues concerning patient safety risks, and regulatory agencies might have to monitor these new kinds of issues in the future. In the second example, new ethical issues related to the patient-doctor relationship may arise, further to the lack of explanation or transparency in the process. These examples are hypothetical. However, they might suggest that one can expect new legal or ethical challenges that future strands of research in health law or medical ethics might need to study.

The 'data' of the Data Act proposal. About 'inferred or derived' data – The proposal may also entail interpretative uncertainties as regards the scope of 'data'. The proposal sets obligations for

---

[372] See EDPB-EDPS (n 371) 11: 'the definition of "data holder" should be further clarified'.

[373] See EHDS proposal, art 2(2)(y): 'data holder' means any natural or legal person, which is an entity or a body in the health or care sector, or performing research in relation to these sectors, as well as Union institutions, bodies, offices and agencies 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, through control of the technical design of a product and related services, the ability to make available, including to register, provide, restrict access or exchange certain data'.

[374] See sec 3. See also Teodora Lalova-Spinks and Daniela Spajic, 'The broadening of the right to data portability for Internet-of-Things products in the Data Act: who does the act actually empower? (Part I)' (*CiTiP Blog*, 16 June 2022) <https://www.law.kuleuven.be/citip/blog/the-broadening-of-the-right-to-data-portability-for-internet-of-things-products-in-the-data-act-part-i/>.

[375] For a similar example, see ITI, 'ITI Comments to the Data Act Proposal' (13 May 2022) 5 < https://www.itic.org/documents/europe/Final-ITIDataActComments.pdf> accessed 9 September 2022.

[376] Cf sec 16.4 concerning inferred data. However, even if inferred data are excluded from the scope (in the recitals), it could still be the case that data relevant to the execution of a certain test revealing details about the test could not qualify as 'inferred'.

'generated' data, and it specifies that information derived or inferred should not be considered in the scope of the proposal (Recital 14).[377] The proposal does not define 'inferred or derived data'. In data protection law, inferred data 'are data created by the data controller on the basis of the data 'provided by the data subject'[378]. The EHDS proposal suggests that inferred data are, for example, 'diagnostics, tests, medical examinations'.[379]

On the one hand, excluding inferred data in the Data Act proposal may seem appropriate for certain kinds of inferred data – such as diagnostics or tests – so that third parties do not have access outside of health research purposes. [380] The EHDS proposal includes inferred data in its scope. Therefore, patients would still, in principle, have the right to access these data following the EHDS framework (which is oriented towards strengthening the rights of natural persons in relation to the availability and control of their electronic health data). On the other hand, some questions may arise regarding the inclusions or exclusions of other kinds of (non-personal?)[381] data, such as synthetic data. Would synthetic data[382] constitute 'inferred data', and if yes, would they be excluded from the scope of the Data Act? As known, in the healthcare sector, synthetic data may be useful for the purposes of developing AI-based medical devices. [383] They are, for example, deemed helpful in mitigating the paucity of annotated medical data. [384] Often, their use is made to overcome problems of (under)representation of patient populations in training data sets of technologies.[385] The more data sets present flaws in this respect, the more the risk of a misdiagnosis – to continue the example.[386]

While the EHDS proposal could, in principle, allow– although with different actors – the sharing of synthetic data if considered as inferred,[387] it would be necessary to know how where synthetic data stand in this category to avoid uncertainties in the future application of this piece of legislation.[388]

## 16.4. The interplay of the Data Act proposal with other (medical device) laws

[377] See sec 3. See also, Lalova-Spinks and Spajic (n 353).

[378] Article 29 Working Party, 'Guidelines on the right to data portability under Regulation 2016/679, WP242 rev.01' (2018), 10.

[379] EHDS proposal, rec 5.

[380] This choice may depend on the fact that the proposal is grounded on the ratio to open secondary markets for IoT data and minimise adverse effects on markets. see Matthias Leistner and Lucie Antoine, 'IPR and the use of open data and data sharing initiatives by public and private actors' (European Union, 2022) <https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2022)732266> accessed 9 September 2022.

[381] The nature of synthetic data as personal or non-personal data is discussed in the literature (see as an example, Theresa Stadler and others,, 'Synthetic Data – Anonymisation Groundhog Day' (*ArXiv,* 2020) <https://arxiv.org/abs/2011.07018> accessed 9 September 2022 – however, the discussion falls beyond the scope of this article.

[382] On the notion of synthetic data, see EDPS, 'Synthetic Data' (*EDPS,* n.d.) https://edps.europa.eu/press-publications/publications/techsonar/synthetic-data_en#:~:text=Synthetic%20data%20is%20artificial%20data,undergoing%20the%20same%20statistical%20analysis> accessed 9 September 2022.

[383] See, for example, Richard J Chen and others, 'Synthetic data in machine learning for medicine in healthcare' (2021) 5(6) Nature biomedical engineering.

[384] ibid.

[385] The issue is broad and exceeds the scope of the paper. For relevant remarks in the matter, see Eduard Fosch-Villaronga and others, 'Accounting for diversity in AI for medicine' (2022) 47 November 2022 105735 Computer Law & Security Review.

[386] The usual example: cancer spotting images from the study by Esteva and others reviewed by Zou and Schiebinger. See Andre Esteva and others, 'Dermatologist-level classification of skin cancer with deep neural networks' (2017) 542(7639) Nature; James Zou and Londa Schiebinger 'AI can be sexist and racist—It's time to make it fair' (2018) 559(7714) Nature.

[387] EDHS proposal, rec 5.

[388] It is worth to note that these uncertainties may be further exacerbated from the formulation 'should not', (which is an hypothetical tense), and the fact that this aspect is treated in a recital, instead of an article.

The contribution by Lalova-Spinks highlighted that health data sharing would be concerned not only by the Data Act proposal but also by other pieces of legislation, such as the GDPR and the European Health Data Space proposal. The remarks and the tensions they identified[389] will also be relevant to medical devices since the GDPR, as well as the Data Act and the EHDS, once approved, would apply to them.

The Data Act proposal may be relevant to cybersecurity regulation. As noted elsewhere, cybersecurity – including healthcare cybersecurity – has been regulated in the EU through different pieces of legislation, both of vertical and horizontal reach.[390] Also, the Data Act proposal could offer rules relevant to medical devices cybersecurity. These are contained in Chapter V of the proposal concerning making data available to public sector bodies and union institutions, agencies or bodies based on exceptional need.[391] Let us read Articles 14-15 of the proposal with recital 57 of the Data Act proposal conjunctively. According to these, an exceptional need to use data may exist, among others, where the data requested is necessary to respond to a public emergency (Article 15(1)a) or where the data request is necessary to prevent it or to assist the recovery from it (Article 15(1)(b)). Recital 57 of the proposal seems to assert that *major cybersecurity incidents* should be considered a public emergency.

The following example of a major[392] cybersecurity incident may support the discussion:

> Example: A large healthcare provider is targeted by a cyberattack that happened through ransomware inside a DICOM file image of an MRI scan.[393] Fastly, the DICOM file infects the doctor's computer and then reaches the hospital's Picture Archiving and Communication System (PACS). Then, the ransomware proliferates to the whole hospital network shutting down all the operations and causing data and service unavailability.
>
> Consequence: The healthcare provider or the manufacturer of the MRI scan might now be subject to the obligation to make certain data available to a public sector body – if they request them, to assist the recovery from this cybersecurity incident or to prevent another one happens to another hospital's medical device.

The example above shows the relevance of the Data Act proposal to cybersecurity incidents. Following this situation, some interpretative uncertainties may arise. First: since the recital mentions 'major' cybersecurity incidents, issues may occur around the word 'major'. How to understand whether an event is major and which thresholds distinguish them from non-major cybersecurity incidents? It may be important to clarify this aspect since the public sector body will have to demonstrate the

[389] See art 5 Data Act proposal and art 20 GDPR, having regard especially to the processing legal bases. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L 119/1 (GDPR).

[390] These pieces of regulation include the MDR/IVDR for their safety requirements, as well as the GDPR, the NIS Directive, or the Cybersecurity Act. see Elisabetta Biasin and Erik Kamenjašević, 'Cybersecurity of Medical Devices. Regulatory challenges in the EU' in Glenn I Cohen and others (eds), *The Future of Medical Device Regulation: Innovation and Protection* Cambridge University Press 2022.

[391] As better illustrated in sec 8, see supra.

[392] Caveat: The example in this use case is at the best of our guesses. As highlighted *infra*, evaluating whether a cybersecurity incident is 'major' may require further clarification.

[393] DICOM file is a recognised vulnerability in the security area, see Jessica Davis 'DICOM Flaw Enables Malware to Hide Behind Medical Images' (*HealthITSecurity,* 18 April 2019) <https://healthitsecurity.com/news/dicom-flaw-enables-malware-to-hide-behind-medical-images> accessed 9 September 2022; Benoit Desjardins and others, 'DICOM Images Have Been Hacked! Now What?' 2020 214(4) American Journal of Roentgenology.

exceptional need,[394] and data holders should be able to decline the request if this requirement is not met.[395]

More uncertainties could be related (again) to the nature of data that should be shared. Once again, we come back to the 'inferred data' problem. In this specific case, one could debate as to whether a DICOM file is inferred data since it contains medical imaging – and thus tests and medical examinations. Therefore, in this specific case, the public sector body could receive data but not the specific data containing the malware that caused the major cybersecurity incident [sic]. Some stakeholders[396] also noted that the proposal does not specify whether security data (such as logs and passwords) are within the proposal's scope. This contribution cannot analyse in detail this aspect for reasons of space. However, it is crucial to raise this point in the public discussion while paying attention to the role of security, privacy and fundamental rights when evaluating the values at stake.

Finally, Article 16 of the proposal specifies that the rights from chapter V shall not be exercised by public sector bodies and Union institutions, agencies and bodies to carry out activities for the prevention, investigation, detection or prosecution of criminal or administrative offences or the execution of criminal penalties, or for customs or taxation administration. It remains thus to be analysed in detail how these could align with cybersecurity emergencies, especially when it comes to preventing them.

## 16.5. Conclusion

This use case aimed to highlight possible issues stemming from the Data Act proposal, having regard to its definitions and the possible interplays with existing legislation. As highlighted through the use case of medical devices, some interpretative issues could arise.

To help the EU legislator in addressing them, below are some policy recommendations:

- Data holders: Clarify 'through control of the technical design of the product and related services*;*
- Major cybersecurity incidents (public emergencies). Clarify the meaning of 'major' cybersecurity incidents and consider more broadly the potentials of including cybersecurity within the scope of the Data Act.
- 'Inferred data': Clarify the meaning of 'inferred data'.

In addition, research might be called to analyse the current provisions of the Data Act proposal or challenges that might arise from them in the future. These may include new ethical challenges, or legal tensions possibly brought by the interplay between the EHDS proposal and the GDPR or with (cyber)security legislation.

[394] Data Act proposal, art 17(1)(b).
[395] Ibid, art 18(2)(b).
[396] See ITI, (n 358).

# 17. Conclusions of the White Paper – Charlotte Ducuing,[397] Luca Schirru,[398] Ella De Noyette,[399] Thomas Margoni[400]

The conclusions start with an overview of the substantive sections discussed in the White Paper. This is followed by a list of recommendations that we hope may result as useful guidance for policy and law makers. We conclude with some general reflections on the state of EU law in the field, in particular in relation to data portability, European Data Spaces, independent administrative enforcement authorities, the role of data intermediaries and the international context.

## 17.1. Summary of the main findings and recommendations

The **introduction** of the White Paper contextualised the theoretical framework within which the analysis has been developed. This included the broader policy structure of the EU Data Strategy and the role of the Data Act and other instruments of EU Data Law. The introduction finally identified four general recurring themes in the Data Act and, more generally, in the public discourse regarding the EU data strategy: (1) Fixing well-known issues in data markets: A pragmatic approach; (2) Unleashing the value of privately held data: Data Spaces; (3) Innovative approaches: data in the public interest, data sharing and data co-generation; and (4) Regulatory interfaces: The Data Act and other areas of information law.

**Sec. 2** of the White Paper focused on IoT data access and sharing obligations as regulated in Ch 2 of the Data Act. It focused on so-called defensive and positive facets of 'data control' that the Data Act is expected to guarantee for the user of an IoT product or related service.

**Sec. 3** of the White Paper analysed the topic of data portability contained in the Data Act in relation to other legal instruments, such as the GDPR, the DGA and the proposal for a European Health Data Space Regulation, with a focus on the empowerment of individual rights.

**Secs. 4 and 5** of the White Paper examined Chapter III of the Data Act, assessing, on the one hand, the appropriateness of the FRAND terms as conditions for future obligations to make data available (Article 8) and the interpretative uncertainties of the provisions on technical protections measures (Article 11), on the other hand.

**Sec. 6** of the White Paper builds a conceptual bridge between Chapters III and IV of the Data Act and offers an overview of the B2B sharing and access rules in the cases of contractual (Chapter III) and statutory (Chapter IV) obligations to make data available and the role of the fairness test of Article 13.

**Secs. 7-9** of the White Paper discussed Chapter V of the Data Act. First, Sec. 7 dealt with the general concept of B2G data sharing. It analysed the "what, who, when and how" of these obligations and raised a (first) number of questions on the scope of B2G sharing. Then, Sec. 8 dived into the 'exceptional need' concept. Finally, Sec. 9 provided a case study, setting out the need for data-sharing for smart city development and the possibilities the Data Act creates.

[397] Doctoral researcher at Centre for IT & IP Law (CiTiP), KU Leuven, Belgium.
[398] Postdoctoral researcher at Centre for IT & IP Law (CiTiP), KU Leuven, Belgium.
[399] PhD researcher at Centre for methodology of law and Centre for IT & IP Law (CiTiP), KU Leuven Kulak, Belgium.
[400] Research Professor of Intellectual Property Law at the Faculty of Law and Criminology, KU Leuven.

**Sec. 10** of the White Paper focused on a specific aspect of Chapter VI, that is, the obligations of data processing service providers to remove obstacles to and assist their users in effective switching between providers, or in other words, to the 'right to switch'.

**Secs. 11-12** of the White Paper discussed Chapter VII and the international access and transfers of data. Article 27 provides safeguards against unlawful access and transfers to non-EU countries, prohibiting certain transfers and obliging the providers to take 'all reasonable measures' to prevent those transfers. While the first contribution of this section gave a general overview of the Article, the second contribution discussed similarities and differences with the existing regulatory landscape, in particular, the GDPR and the DGA.

**Sec. 13** of the White Paper covered Chapter IX of Data Act on enforcement measures. The Data Act requires Member States to establish two new types of enforcement authorities: the 'dispute settlement bodies' and the respective 'competent authorities' and grants supplementary competences to the 'European Data Innovation Board', already set up by the DGA.

**Sec. 14** of the White Paper discussed Chapter X of the Data Act, which offers a much-needed clarification on the relationship between IoT data and the sui generis database right (SGDR), in particular by 'clarifying' that the SGDR does not apply to IoT data.

**Sec. 15** of the Data Act addressed the complex relationship between the Trade Secrets Directive and the Data Act. Both instruments try to facilitate information sharing, but the TSD does this by protecting the shared information rather than obliging the sharing itself.

**Sec. 16** of the White Paper develops a case study on the relationship between the Data Act and medical devices. The Section considered the definitions of 'data holder', 'user', and 'data' in a complex medical device data sharing scenario and identified interpretational difficulties. As health data is also a concern of other legislative initiatives, such as the GDPR, the EHDS, the (In-Vitro) Medical Device Regulation, the NIS Directive and the Cybersecurity Act, part 16 also discussed the interplay with these initiatives.

## 17.2. Priority recommendations

The White Paper developed a detailed article-by-article (or Section) analysis of the Data Act proposal. In the below table we summarise the main recommendations that the authors of each section have formulated with the intention of offering an external and independent scientific input to the law-making process. They are grouped into four main categories: Terminological clarification, Synergy with other laws, Internal harmonisation/classification, addition/removal of obligation.

| Type of recommendation | Chapter of the Data Act Proposal | Recommendation |
|---|---|---|
| **Clarification** | Chapter I | In the definition of 'Data holders': Clarify the exact meaning of 'through control of the technical design of the product and related services'. |
| **Clarification** | Chapters I and V | Consider removing public authorities from the definition of "data holder" (of the Chapter 5) to clarify the "B2G" and "G2G" frameworks. |
| **Clarification, improvement** | Chapter II | Clarify and ensure the downstream effect of Article 4(6), second sentence and clarify that the data portability right under Article 5 is not subject to exhaustion. |

| | | |
|---|---|---|
| **Internal harmonisation** | Chapter II | Regulate further the alignment between the data 'offer' by the data holder and the data 'demand' by the third party chosen by the user under Article 5, by laying down, for instance, specific transparency requirements to the benefit of chosen third parties. |
| **Clarification** | Chapter III | FRAND terms should be clarified in many aspects, including the subject matter of FRAND terms and the compensation (in particular, whether data are covered or not) and what is meant by 'making data available'. |
| **Removal of an existing obligation, improvement** | Chapter III | Article 8(6) should be object of a careful re-drafting as it is currently not well coordinated both taxonomically and systematically with the other provisions and the Data Act and of the TSD. |
| **Improvement, simplification** | Chapter V | Given the close relationship between response, prevention and recovery of public emergency, the differences in the respective legal regimes might be unnecessary (that is, the requirement of "limited in time and scope" in article 15(b) and compensation in article 20). |
| **Clarification** | Chapter V | In relation to "major cybersecurity incidents (public emergencies)": Clarify the meaning of 'major' cybersecurity incidents and consider more broadly the potentials of including cybersecurity within the scope of the Data Act. |
| **Synergy with other laws, concepts and bodies** | Chapter VI | Regulate the interface between Chapter VI and the Digital Content Directive, for example, based on sui generis rules concerning the conformity requirements for switching. |
| **Clarification** | Chapter VII | Clarify the legal nature of the opinion of the competent body or authority on whether the conditions for non-personal data access/transfer are fulfilled and in particular whether such opinion is binding or not. |
| **Synergy with other laws, concepts and bodies** | Chapter IX | Insofar as competent authorities shall be established by member States, regulate further the conditions in which they shall cooperate between the respective enforcement authorities. |
| **Removal of an existing obligation** | Chapter IX | Remove the obligation of competent authorities and DPAs to 'seek consistency' when enforcing the Data Act. |
| **New obligation** | Chapter X | In order to give it full and clear legal effect, the obligation contained in Recital 63 should be moved and/or restated in the main body of the Act (i.e., as an Article). |
| **Clarification** | Chapter X | Remove the first part of Article 35 and place it in Rec. 84 to help eliminating any possible doubt relating to the scope of the exclusion. |
| **Synergy with other laws, concepts and bodies** | Chapter X | Clarify that "For the purpose of Article 7 Database Directive, IoT data as defined in the Data Act are created data and, therefore, as such have never been object of SGDR protection". |
| **Clarification** | Data Act | Consider exploring (informal) procedural guarantees to protect the user against artificial blocks of sharing requests by the data holder in relation to ex ante v. ex post determination of Trade Secret. |

| | | |
|---|---|---|
| **Synergy with other laws, concepts and bodies** | Data Act | The terminology employed to enshrine the new versions of the right to data portability under the Data Act and EHDS proposals shall be unified, and the legal and technical interoperability between the various applicable laws shall be guaranteed. |

## 17.3. Summary of findings: Final consideration on the state of EU Data Law

This section develops some final considerations on the current state of EU Data Law, focusing on data portability, European Data Spaces, independent administrative enforcement authorities, the role of data intermediaries and the international context.

### 17.3.1. Data portability: potential and (over-)expectations

Data portability is mentioned no less than 22 times in the Data Act proposal and operationalised in two different legal regimes. First, IoT product users are granted a 'data portability right' (Chapter II) enforceable against the 'data holder', mainly the IoT product manufacturer, (see sections 2 and 3). Second, data portability constitutes an enabling tool for switching as per Chapter VI of the proposal (see section 10), alongside the portability of other assets. Closely related to interoperability, data portability – and more generally, the portability of the 'digital assets' of data processing service customers – constitute an objective for developing open interoperability specifications and European standards.[401] Both occurrences undoubtedly build upon the data portability right granted to data subjects by the GDPR under the circumstances laid down in Article 20,[402] while data portability rights can also be found in other legislative frameworks.

The notion of data portability is remarkably undefined, both in the GDPR and in the Data Act proposal, for example. Data portability is generally designed to empower its beneficiaries with respect to 'their' data and to make markets more competitive. This being, many differences can be observed concerning the scope, beneficiaries, and purposes, among others. In relation to the Data Act proposal, two main striking differences can be observed between data portability under Chapter II and VI, respectively. First, under Chapter II, data portability constitutes a self-standing right, while data portability is 'only' a component of the more general regime enabling switching under Chapter VI. Second, the respective objectives, and thus magnitude, are different. Data portability enables data processing service customers to switch to a new provider, which results in the termination of the contract. In Chapter II, the data portability right is viewed by the EC as a non-exhaustible right for IoT product users. Users may exert their data portability right several times, for different purposes and with different third parties. The data portability right in Chapter II is not meant to constitute a prerequisite for the termination of the contract with the data holder. On the contrary, it can be strategic for the user to retain the relationship with the data holder as a continuous data provider. [403]

[401] 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 (Data Act proposal), art 29(1)(b) and art 29(2)(b) and (c).

[402] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L 119/1 (GDPR), art 20.

[403] On this, see also Charlotte Ducuing, 'An Analysis of IoT Data Regulation under the Data Act Proposal through Property Law Lenses' (2022) CiTiP Working Paper 2022, sec 4 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4225027> accessed 7 October 2022.

The Data Act proposal shows that data portability has become a key concept in the Commission toolbox given its alleged ability to fix most (if not all all) market failures in the digital environment. However, the concept of data portability did not receive a unique definition across the Data Act and in fact it carries different meaning depending on the specific provision.[404] This may lead to legal uncertainty and to the detriment of the efficacy of some of the key provisions of the Data Act.

As argued, 'data portability' is gaining traction as a tool able to fix market failures and to empower the respective beneficiaries. However, as it has been effectively argued, data portability will only deliver on expectations – if at all – provided that interoperability is guaranteed.[405] This essential lesson learned from the application of the data portability right under the GDPR, shifts the focus from portability to the regulation of interoperability as a key factor. Additionally, it may also be necessary a word of caution about over-expectations from data portability. It is arguable, if not likely, that the data portability right granted to users of IoT products under Chapter II of the Data Act will not suffice alone to solve *all* the associated market failures and to genuinely enable aftermarket providers to access and use the data that they need. This calls for further initiatives, possibly as part of additional sectorial regulatory interventions, in the field of European Data Spaces.

Finally, another element of attention should be added in relation to the risk of 'greenwashing' the Data Act. In particular, the regulation of IoT under Chapter II of the Data Act is motivated by the ambition to support the "development of digital and other services protecting the environment, health and the circular economy, in particular through facilitating the maintenance and repair of the products in question".[406] It is undeniable that the maintenance and repair of products is generally conducive to the circular economy transition. However, the Data Act 'bets' in a way on a proactive role of the user, which remains a plausible eventuality in need of empirical confirmation. It is thus clear that the Data Act itself does not suffice to enable the making available of the required data to IoT product aftermarket providers. In this context, circular economy-dedicated data production and sharing obligations, for instance as part of the new Ecodesign Regulation proposal,[407] shall be scrutinized and the compatibility between the two legal instruments shall be ensured. Finally, a provocative question should be asked, in view of the alarming messages stemming regularly from both the Intergovernmental Panel and Climate Change (IPCC) and the Intergovernmental Science-based Platform on Biodiversity and Ecosystem Services (IPBES). Given the magnitude of the climate and biodiversity issues, are data sharing obligations under the Data Act fit for purpose? While data reuse can undoubtedly play a role in the circular economy transition, it may in certain cases be found that more sweeping solutions are preferable.

### 17.3.2. What law for the data spaces?

In the eyes of the Commission, the Data Act constitutes the cornerstone of upcoming EU Data (Spaces) Law. It will be complemented by sector- or domain-specific regulations for data spaces, towards the realisation of a single market for data. The Data Act does already provide several connections with

[404] Data portability is for example defined neither in the GDPR, nor in the FFNPDR nor even in the Data Act.

[405] See among others, Inge Graef, Martin Husovec, and Nadezhda Purtova, 'Data Portability and Data Control: Lessons for an Emerging Concept in EU Law' (2018) 19 German Law Journal, 1386, 1387.

[406] Data Act proposal, rec 14.

[407] Commission, 'Proposal for a Regulation of the European Parliament and of the Council establishing a framework for setting ecodesign requirements for sustainable products and repealing Directive 2009/125/EC' COM/2022/142 final (Ecodesign Regulation proposal).

existing and future regulations. Chapter III regulates the conditions with which data holder shall comply when bound to make data available, for example as a result of data space-specific regulations (legal aspects). Additionally, Chapter VIII lays down the framework for the future regulation of interoperability necessary for the smooth operation of data spaces (technical aspects). Both Chapters III and VIII are expected to provide the foundations for data spaces, and especially for their data space-specific regulation. Against this background, the question arises what 'the law of data spaces' should look like.

In its European Data Strategy of 2020, the Commission provides a conceptual definition of what 'law of data spaces' it aims for:

> The Commission's approach to regulation is to create frameworks that shape the context, allowing lively, dynamic and vivid ecosystems to develop. Because it is difficult to fully comprehend all elements of this transformation towards a data-agile economy, the Commission deliberately abstains from overly detailed, heavy-handed ex ante regulation, and will prefer an agile approach to governance that favours experimentation (such as regulatory sandboxes), iteration, and differentiation.[408]

To the best of our knowledge, this constitutes the first occurrence of the term 'agility' applied to law, or more generally to 'governance', by the Commission. 'Agility' then finds other complementary terms such as experimentation, iteration and differentiation. An agile governance is put forward against the background of the characterisation of data spaces as 'lively, dynamic and vivid *ecosystems'*. The issue at stake is indeed that not all constitutive elements can be fully comprehended ex ante.

The question that logically arises is how to move to an 'agile governance' for data spaces while keeping up with legal foundational principles, such as legal certainty, democratic values and the rule of law. CiTiP investigated this question in its yearly Leuven AI Law & Ethics Conference (LAILEC), edition 2022. The panel 'Governance of data spaces: Collaboration, experimentation, agility and adaptivity' explored this theme focusing precisely on the notion(s) of agile regulation, the relevance of regulatory experimentation, the challenge of adaptability and the potential of a form of circular law, where the law would become an integral part of the development process of data spaces.[409] It emerged that 'agile governance' constitutes a continuation of the 'better regulation agenda'.[410] 'Agile governance' can also be related to the 'principle of innovation' that the Commission applies to its own regulatory activities.[411] Agility, experimentation and innovation do indeed come from the provision of goods and services. The use of such terms with reference to the law or more generally to 'governance' and

---

[408] Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: "A European strategy for data" COM(2020) 66 final, sec 5.

[409] See KU Leuven, 'Life-cycle regulation of Data and AI, Tackling dynamicity and responsibility in complex ecosystems', Panel 3.2 (*LAILEC 2022*, 28 March 2022), <https://www.law.kuleuven.be/citip/en/citip-conferences/lailec/lailec-2022/programme-1/programme-day-1>).

[410] On the various non-legislative initiatives of the Commission on the 'Better Regulation' agenda, see Commission, 'Better Regulation: why and how' <https://ec.europa.eu/info/law/law-making-process/planning-and-proposing-law/better-regulation-why-and-how_en> accessed 18 October 2022.

[411] The Council of the European Union made an explicit connection between the 'innovation principle' and 'an agile, innovation-friendly, future-proof, evidence-based and resilient regulatory framework […]' in the Conclusions on Council, 'Regulatory sandboxes and experimentation clauses as tools for an innovation-friendly, future-proof and resilient regulatory framework that masters disruptive challenges in the digital age' (13026/20, General Secretariat of the Council, 2020).

'regulation' appears to assimilate the latter with goods and services.[412] This is viewed as a means to adapt the law to its object, in this case data spaces viewed as dynamic and fluid ecosystems, and more generally to keep pace with innovation.[413]

Nevertheless, it remains to be seen how, concretely, data spaces will operate and, relatedly, how the law will contribute to such operation. Inspiration can be drawn from previous experiences.

It can be observed how signs of dynamicity and a form of circularity of the law can be discerned in the law-making process for the regulation of 'switching' between data processing service providers, for example.[414] The law-making process for the regulation of 'switching' between data processing service providers displays interesting regulatory features, namely a shift to a more dynamic or even circular nature of the law and of the law-making as a practice. The lawmaker, and especially the Commission, appears to picture itself not so much vertically as an overhanging maker of the (market) rules but, to a certain extent, horizontally as an entity playing in the same arena as businesses, albeit with its own objectives and tools. This can be illustrated as follows. First, the Free-Flow of Non-Personal Data Regulation mandates both the Commission and businesses to team-up and co-regulate the sector. Second, the Commission has visibly opted for elements of a dynamic (or else circular – or 'agile'?) law-making process whereby only a lack of voluntary implementation or adoption of the sought regulatory mechanisms by businesses triggers in the Commission the need for adoption of a new, more stringent, intervention.

Somehow departing from the classical hierarchy of norms, we can observe that, with both the FFNPDR and the ensuing "facilitation of the development of self-regulatory codes of conduct",[415] the EU lawmaker was aiming to set incentives for businesses to self-regulate. Because the initiative failed, the Commission eventually used the 'stick' of heavy hand regulation with Chapter VI of the Data Act, which appears to put a stop to the 'dynamicity' of the law.

Close interactions between the lawmaker and businesses are recurrent with EU law and not specific to just the regulation of data processing service providers. Elements of a 'dynamic' or 'agile' law could possibly be taken a step further for the regulation of data spaces, following the ambition of the Commission. A proposed visual representation is offered below as Fig. 4.

[412] On this, see Charlotte Ducuing, 'A Legal Principle of Innovation? Need for an Assessment against the Principle of Democracy' (2022) Law, Innovation and Technology, 20,21 <https://doi.org/10.1080/17579961.2022.2113667> accessed 18 October 2022.

[413] For a conceptual characterisation of the innovation principle and on the possibly encroachment on democracy, see Ducuing (n 404).

[414] See sec 10.

[415] FFNPDR, art 6.

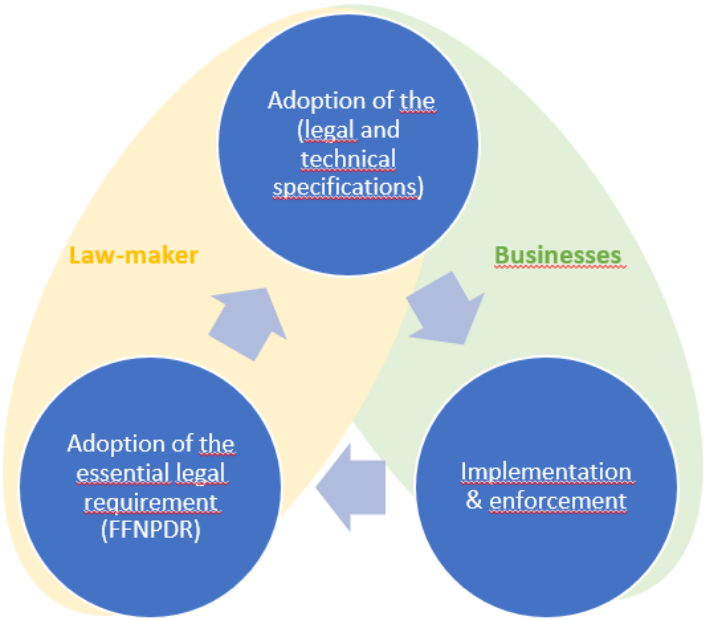


**Fig. 4: Towards circular legislation for the free-flow of non-personal data**

With the double objective to, first, enable the law to keep pace with innovation and, second, to allow experimentations, regulatory sandboxes have become a major theme in the field of law and technology. It is therefore no surprise that regulatory sandboxing is expressly referred to in the European Data Strategy.[416] Regulatory sandboxing and innovation hubs have been piloted in the field of 'FinTech'.[417] More recently, the AI Act has aimed to foster use of regulatory sandboxes, viewed as a novel form of regulatory oversight and a safe space for experimentation, in order to support innovation.[418] Regulatory sandboxes should essentially

> support innovators in preparing for the deployment of AI-related innovations (including, preparing for compliance with the AI Act) while, on the other, enabling regulators (namely, both the lawmaker and, where appropriate, administrative and regulatory authorities) to prepare for the advent of (and especially, get to understand) AI innovations on the market.[419]

The role of enforcement authorities is thereby core to the operation of regulatory sandboxes.[420] A major issue with both AI and data, is that they are often governed by many different legislations, both at EU and national levels. This makes it very difficult to create regulatory 'safe harbours', although they

[416] Commission, 'A European Strategy for Data' (n 409), sec 5.A.

[417] For a thorough analysis, see Radostina Parenti, 'Regulatory Sandboxes and Innovation Hubs for FinTech - Impact on Innovation, Financial Stability and Supervisory Convergence', Study for the committee on Economic and Monetary Affairs, Policy Department for Economic, Scientific and Quality of Life Policies (Luxembourg: European Parliament, 2020).

[418] Commission, 'Proposal for a Regulation of the European Parliament and of The Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts', COM/2021/206 final, art 53 and rec 71.

[419] Ducuing (n 404) 12.

[420] In this respect, Ducuing warns against that this may affect the statutory role of enforcement authorities, Ducuing (n 385) 12–13.

constitute a key success factor for regulatory sandboxes.[421] It remains therefore to be seen how 'the law of data spaces' could overcome this challenge so regulatory sandboxing could possibly be enacted.

A final observation relates to policy prototyping as an alternative type of interaction between policy- and law-makers on the one hand, and stakeholders on the other. Policy prototyping can be viewed as "a form of inversed regulatory sandboxing", whereby different stakeholders "discuss rules before they enter into force" based on a "field-testing phase of new draft rules before finalising and adopting them".[422] Such method has for example been used by the Flemish Knowledge Centre for Data & Society to evaluate certain provisions of the AI Act.[423] Dheu, De Bruyne and Ducuing suggest that policy prototyping could serve to substantiate general concepts[424] used in the recent AI Liability Directive proposal[425] and revised Product Liability Directive proposal.[426] Policy prototyping could also similarly be envisaged as a means to substantiate concepts such as 'FRAND terms' under the Chapter III of the Data Act.

### 17.3.3. A renewed theory of IAEAs

The Data Act may be seen as constituting an instance of the broader trend of the EU lawmaker to recourse to dedicated independent administrative enforcement authorities. As section 13 showed, this is not without considerable consequences. Accordingly, a brief reflection about the need for a renewed theory of the role and legitimacy of such authorities in the EU follows.[427]

Independent administrative authorities have traditionally been found to have an added value, compared to the standard role of the judiciary in adjudicating controversies, in particular where enforcement requires specialistic economic, technical, legal expertise. Authorities are often granted far-reaching - possibly including ex ante or even, to a minor extent regulatory, - competences. However, compared to the judiciary, their jurisdiction is limited to a certain scope of application, whether sectorial regulation (such as liberalised network industries) or a given branch of law (such as competition law or, respectively, personal data protection law). For this reason, Frison-Roche calls them "powerful cyclops".[428] In short, the added value of such authorities as enforcers lies mainly in their expertise and swiftness.

However, as becomes clear with the Data Act and by the DGA, independent administrative enforcement authorities are increasingly requested to cooperate one with the other as their respective

---

[421] Vladislav O. Makarov and Marina L. Davydova, 'On the Concept of Regulatory Sandboxes' in Elena G. Popkova and Bruno S. Sergi (eds) *"Smart Technologies" for Society, State and Economy* (Springer 2021), 1014–20.

[422] Orian Dheu, Jan De Bruyne, and Charlotte Ducuing, 'The European Commission's Approach To Extra-Contractual Liability and AI – A First Analysis and Evaluation of the Two Proposals' (2022) CiTiP Working Paper Series, 42-43 < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4239792> accessed 18 October 2022. ; Thomas Gils, Koen Vranckaert, and Brahim Benichou, 'Exploring Policy Prototyping – Some Initial Remarks' (*CiTiP Blog,* 2021) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3885571>.

[423] See Knowledge Centre Data & Society, 'Policy prototyping – AI act' (18 March 2022) <https://data-en-maatschappij.ai/en/news/policy-prototyping-ai-verordening> accessed 18 October 2022.

[424] Dheu, De Bruyne, and Ducuing (n.423) 42–43.

[425] Commission, 'Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive)' [2022] COM (2022) 496 final, 3.

[426] Commission, 'Proposal from the European Commission for a Directive of the European Parliament and of the Council on liability for defective products (revised Product Liability Directive proposal or revised PLD proposal)' [2022] COM/2022/495 final.

[427] For a similar endeavour in the US, see Sabeel K. Rahman, *Democracy against domination* (Oxford University Press, 2016).

[428] Marie-Anne Frison-Roche, 'L'hypothèse de l'interrégulation', in Marie-Anne Frison-Roche (ed) *Droit et Economie de La Régulation 3. Volume 3: Les Risques de Régulation* , vol. 3 (Presses de Sciences Po, 2005).

scopes of application get increasingly intertwined. Should the Advocate General's conclusions in the *Meta Platforms v Bundeskartellamt* case[429] be followed by the Court, this may require extensive procedural regulation. The Advocate General notes that 'it may fall to the EU legislature to adopt […] clear rules on cooperation mechanisms' between, in this case, DPAs and competition authorities.[430] In the absence of such rules, the Advocate General had to resort to general principles in the Treaties, namely the duty of member States to cooperate in good faith (Article 4(3) TEU)) and the principle of sound administration, to provide guidelines for cooperation.[431] It is argued that such a subtlety will likely not suffice, should cooperation between authorities be taken to the next level as EU Data Law seems to suggest.

Furthermore, this situation undoubtedly affects the swiftness of enforcement authorities, especially if they are requested to stay proceedings until another 'lead' authority delivers its decision. It could also possibly affect their expertise, as they will increasingly have to consider other legislations. The establishment of independent administrative enforcement authorities implies a prioritisation of the policy at stake. However, where such authorities as established for many policies, including policies that are essentially in tension such as data sharing and personal data protection, it raises the question of which policy is given priority.

Finally, it is arguable that the far-reaching competences that authorities are often granted, could easily impinge on the principle of separation of powers as well as on democracy, as they operate independently from representative institutions.[432] The latter 'downside' is often compensated by alternative consultation mechanisms, so interested parties can participate via their opinion.[433] However, the legitimacy question remains a crucial one, as authorities are granted not only increasing competences, but they are also increasingly requested to arbitrate between different policy objectives.[434] This should remain a crucial warning for the regulation of the digital environment.

### 17.3.4. The role of data intermediaries: Missed opportunity?

Criticisms has already been raised in the literature about the unclear relationship between the DGA and the Data Act.[435] This is particularly the case concerning the role that data intermediaries, governed by the Chapter III of the DGA, could play to facilitate Chapter II of the Data Act.[436]

---

[429] Case C-252/21, *Meta Platforms v Bundeskartellamt*, Opinion of AG Rantos, paras 28-33.

[430] Ibid, para 29.

[431] Ibid, para 28.

[432] See, for example, Jacques Chevallier, 'Autorités administratives indépendantes et État de droit' (2016) 2 Civitas Europa, 143.

[433] Libby Maman, 'The Democratic Qualities of Regulatory Agencies'(2022) 50 (4) Policy & Politics, 461 <https://doi.org/10.1332/030557321X16490875448288> accessed 18 October 2022.

[434] This is essentially the issue at stake with the cases German Federal Constitutional Court (BVerfG), Judgment of the Second Senate of 5 May 2020 – 2 BvR 859/15, following CJEU, 11 December 2018, C-493/17, ECLI:EU:C:2018:1000 ('Weiss and others' case) on the delineation of the mandate of the European Central Bank (ECB).

[435] See, for example, Peter Georg Picht, 'Caught in the Acts: Framing Mandatory Data Access Transactions under the Data Act, further EU Digital Regulation Acts, and Competition Law' (2022) Max Planck Institute for Innovation and Competition Research Paper No. 22-12, 30-32 < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4076842> accessed 18 October 2022.

[436] Peter Georg Picht, 'Caught in the Acts: Framing Mandatory Data Access Transactions under the Data Act, further EU Digital Regulation Acts, and Competition Law' (2022) Max Planck Institute for Innovation and Competition Research Paper No. 22-12, 30-32 < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4076842> accessed 18 October 2022; Peter Georg Picht and Heiko Richter, 'EU Digital Regulation 2022: Data Desiderata' (2022) 71(5) GRUR International, 395, 398.

The Max Planck Institute Position Paper suggested that data intermediaries could support the further IoT data commercialisation by 'users' (in particular with a view to AI needs for data).[437] More generally, it is not easy to position data intermediaries on the picture of the various stakeholders, whether as the 'chosen third party' (the beneficiary of the data portability right) or as playing yet another role, or both. We formulate the hypothesis that data intermediaries could also play a role as facilitators of the legal regime laid down in Chapter II. The point of the Data Act is to allocate data fairly to the stakeholders. Especially under Chapter II, this implies to navigate the rights and legitimate interests of several stakeholders, particularly within the triangular relationship formed by the data holder, the user and the chosen third party.

A few issues have been discussed in this respect in this White Paper, which could be considered as frictions in data transactions. Sec. 2 discussed the issue of the misalignment between the data generated by the IoT product and the specific needs of a chosen third party. Section 15 discussed the 'ex ante vs ex post' issue concerning the determination of trade secrets. While, in principle, it is for the judge to decide on the qualification of a given information as trade secret (ex post), Chapter II implies that this decision is made ex ante, namely prior to the sharing of data. Similarly, the data holder could also play personal data protection law strategically as a trump card.[438] In all such cases, there is therefore a risk that the data holder pre-empts the decision of which data should be shared and under which conditions, or in other words retains control over the data, which is precisely the main problem that the Data Act aims to tackle.

Such frictions constitute a typical scenario where the coordination by a trustworthy neutral third party, or in other words of a data intermediary within the meaning of the DGA, can be sought.[439] Data intermediaries could indeed curate the data, both legally and technically, to make sure that they can be lawfully reused. These frictions can hardly be dealt on a general and abstract level with by the law itself, as they are very context dependent. This necessarily requires an actor to play an intermediary role, which comes indeed close to a regulatory role.[440] This solution is not without challenges, which may however be considered to a significant extent covered by the stringent regulation of Chapter III of the DGA. The role of data intermediaries may also be found preferable to the situation where the data holder plays this role, with an evident conflict of interest and the risk to water down Chapter II of the Data Act. Calling on data intermediaries to play a facilitating role to the operation of the law is not

---

[437] 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) https://pure.mpg.de/rest/items/item_3388757_4/component/file_3395639/content> accessed 7 October 2022, para 338.

[438] The press release of BusinessEurope (the representative lobby of large companies across the EU) is illustrative of this risk. It states that "It is also very important not to undermine the confidentiality of trade secrets and *to be consistent with the general data protection regulation (GDPR)* […]" (emphasis added), available at https://www.businesseurope.eu/publications/data-act-eu-data-sharing-framework-should-foster-investment. BusinessEurope, 'Data Act: EU data sharing framework should foster investment' (23 February 2022) <https://www.businesseurope.eu/publications/data-act-eu-data-sharing-framework-should-foster-investment> accessed 18 October 2022.

[439] On the need for data governance to reconciliate conflicting interests concerning data, see Maximilian Grafenstein, 'Reconciling Conflicting Interests in Data through Data Governance. An Analytical Framework (and a Brief Discussion of the Data Governance Act Draft, the Data Act Draft, the AI Regulation Draft, as Well as the GDPR)' (2022), HIIG Discussion Paper, HIIG Discussion Paper Series, 8-9 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4104502> accessed 18 October 2022.

[440] On the quasi-regulatory role expected to be played by data intermediaries under Chapter III of the DGA, see Inge Graef and Raphael Gellert, 'The European Commission's Proposed Data Governance Act: Some Initial Reflections on the Increasingly Complex EU Regulatory Puzzle of Stimulating Data Sharing' (2021) TILEC Discussion Paper, sec 3 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3814721> accessed 18 October 2022.

entirely novel. This suggestion has symptomatically been made with respect to data portability.[441] This possibility is also recognised in the Data Governance Act. Recital 27 indeed anticipates that

> Data intermediation services are expected to play a key role in the data economy, in particular in supporting and promoting voluntary data sharing practices between undertakings or facilitating data sharing in the context of obligations set by Union or national law.

Requiring - or at least enabling – data intermediaries to play such a facilitating role, can be related to the comparison made between them and public services or 'public data utilities'.[442] Should the legislature move in this direction, it remains to be seen concretely how the Data Act could be revised so as to include data intermediaries as such facilitators, or at least to enable them to play this role.

## 17.4. The international context

Finally, we offer a very brief outline of policy and legislative developments in the field of data and data-related technologies outside the EU. With no ambition of exhaustiveness nor of substantial comparative analysis, some updates in selected legal systems where we were able to identify recent developments are given. This constitutes an initial observatory point for the approaches that other legal systems adopt within the boarder theme of data regulation. It is indeed clear that data is flowing to and from countries across and outside the EU. It seems likewise arguable that the challenges that the Data Act and the broader EU Data Strategy aim to address are global and thus not confined within the EU borders.

In countries like Brazil, while there is an effort to discuss and build a framework that is adequate for the development of an AI industry and to follow up international trends,[443] the economic use of non-personal data is, still, mostly, governed by laws concerning IP, TS, and unfair competition practices.[444] One of the most anticipated regulatory developments is the AI Bill that is being discussed in the Senate by experts via public hearings.[445] This consultative process of the policy making on data is also seen in India, where recent regulations were made available for public scrutiny. The Draft of the India Data

[441] On the role of intermediaries to support the implementation of data portability, as per the GDPR, see Matteo Nebbiai, 'Intermediaries Do Matter: Voluntary Standards and the Right to Data Portability' (2022) 11 (2) Internet Policy Review <https://doi.org/10.14763/2022.2.1639> accessed 18 October 2022>. This issue was also raised in the context of the ALI-ELI Principles for a Data Economy, concerning the granting of data access or porting rights. The disclosure to a trusted third party is viewed as a means (among others) to protect the rights of others, see Principles 20(2) and 25(2). See also Charlotte Ducuing, 'Data rights in co-generated data': How to legally qualify such a legal 'UFO'? (*CiTiP Blog*, 12 November 2020) <https://www.law.kuleuven.be/citip/blog/data-rights-in-co-generated-data-part-2/>).

[442] On the emergence of data intermediation as a (quasi-)public service activity in the data economy, see Charlotte Ducuing and René Reich, 'Data utility as an enabler of data spaces? The circular economy as a case study' (Presentation at the FSR 11th Annual Conference, Florence, Italy, June 2022). See also Charlotte Ducuing and Rene Reich, '11th FSR Annual Conference Presentation by Charlotte Ducuing and Rene Reich' (29 June 2022) <https://www.youtube.com/watch?v=8DYifJ4SETY> accessed 18 October 2022; Charlotte Ducuing, 'The data economy as a political project - Focus on emerging "data public utilities"', (Data Forum (EuH4D), Leuven, March 2022) <https://euhubs4data.eu/wp-content/uploads/2022/04/DataForum_slidedeck-all.pdf> accessed 18 October 2022.

[443] Some of the main bills in the Brazilian Senate addressing AI issues are the following: 5051/2019, 21/2020 and 872/2021. The translated texts can be found at https://legis.senado.leg.br/comissoes/comissao?codcol=2504.

[444] See, for example, Law n 9.279/96 (Brazilian Industrial Property Law)

[445] A 'Committee of jurists responsible for subsidizing the preparation of a substitute draft for the bills on artificial intelligence (CJUSBIA)' was created and several public hearings have been carried with the objective of addressing specific issues from different points of view, whether on geographical (that is, different regions) or interest (for example, civil society, academia, industry, public sector) aspects. Brazil, Senate, 'CJUSBIA', Document: '001 - Regulamento Interno, Plano de Trabalho e Cronograma' < https://legis.senado.leg.br/comissoes/comissao?codcol=2504> accessed 21 October 2022.

Accessibility & Use Policy represents an important initiative.[446] Proposed by the Ministry of Electronics and Information Technology, the 'policy aims to radically transform India's ability to harness public sector data for catalysing large scale social transformation' and has as some of its main objectives 'promoting transparency, accountability, and ownership in data sharing & release' and 'facilitating the creation of public digital platforms'.[447] Also open for public consultation (until June 2022), India's National Data Governance Framework Policy is focused on the use of Data by the public administration and 'aims to realize the full potential of Digital Government with the aim of maximising data-led governance and catalysing data-based innovation(...)'.[448] Japan combines interesting approaches, such as a very generous text and data mining exception (thus allowing the extraction of data from protected subject matter to a higher degree than in the EU for instance),[449] with the adoption of a special form of protection for certain data, which was arguably rejected in the EU, namely in Art. 35 Data Act. Through the 2018 revision of the Unfair Competition Prevention Act (UCPA), 'Japan defined valuable data satisfying specific requirements as "Shared Data with Limited Access" (SDLA) and unauthorized acquisition and use, etc. as unfair competition acts (…).'[450] In the US, the most recent initiative that address data-related subject matters is the Blueprint for an AI Bill of Rights released in October 2022 by the White House Office of Science and Technology Policy.[451] As mentioned in the document, this is '(...) a set of five principles and associated practices to help guide the design, use, and deployment of automated systems to protect the rights of the American public in the age of artificial intelligence.'[452] The principles proposed in the Blueprint relate to (i) safety and effectiveness of AI systems, (ii) avoiding algorithmic discrimination, (iii) data privacy, (iv) explainability and transparency and (v) access to 'human consideration and fallback'.[453] Other national initiatives when it comes to data-related policies may be highlighted, as it is the case of the 'AI Next Campaign',[454] 'Big Data to Knowledge',[455] and the

[446] India, Ministry of Electronics and Information Technology, 'Draft India Data Accessibility and Use Policy 2022' <https://www.meity.gov.in/content/draft-india-data-accessibility-use-policy-2022> accessed 19 October 2022.

[447] India, Ministry of Electronics and Information Technology, India Data Accessibility and Use Policy (draft) (February 2022) < https://www.meity.gov.in/writereaddata/files/Draft%20India%20Data%20Accessibility%20and%20Use%20Policy_0.pdf> acessed 17 October 2022.

[448] India, Ministry of Electronics and Information Technology, National data Governance Framework Policy (draft) (May 2022) <https://www.meity.gov.in/writereaddata/files/National%20Data%20Governance%20Framework%20Policy_26%20May%202022.pdf> accessed 17 October 2022.

[449] Copyright Act, 1970 (Act No. 48 of May 6, 1970, as amended up to Act No. 72 of July 13, 2018) (Japan). For a comparative analysis on the different research exceptions in international copyright, see Sean Flynn, Luca Schirru, Michael Palmedo, and Andrés Izquierdo, 'Research Exceptions in Comparative Copyright' (2022) PIJIP/TLS Research Paper Series no. 75, <https://digitalcommons.wcl.american.edu/research/75> accessed 21 October 2022.

[450] Japan, Ministry of Economy, Trade and Industry, Data Utilization & Shared Data with Limited Access <https://www.meti.go.jp/english/policy/economy/chizai/chiteki/data.html> accessed 14 October 2022. Under art. 2(7) of the UCPA 'shared data with limited access' shall be understood as '(…) technical or business information that is accumulated in a reasonable amount using electronic or magnetic means (meaning an electronic form, magnetic form, or any other form that is impossible to perceive without the use of a computer or similar display technology; the same applies in the following paragraph) as information provided to specified persons on a regular basis and that is managed (excluding information that is kept secret).' Japan, IP Policy Office, Economic and Industrial Policy Bureau, Guidance for Data Utilization, Society 5.0, Let's create new value through appropriate data utilization! (2021) < https://www.meti.go.jp/english/policy/economy/chizai/chiteki/pdf/21_0127b.pdf> accessed 14 October 2022.

[451] United States of America, The White House, Blueprint for an AI Bill of Rights: Making automated systems work for the American people (2022) <https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf> accessed 13 October 2022.

[452] Ibid, 4.

[453] Ibid, 5-7.

[454] OECD.AI Policy Observatory, 'AI Next' Campaign <https://oecd.ai/en/dashboards/policy-initiatives/http:%2F%2Faipo.oecd.org%2F2021-data-policyInitiatives-25031> accessed 13 October 2022.

[455] OECD.AI Policy Observatory, Big Data to Knowledge <https://oecd.ai/en/dashboards/policy-initiatives/http:%2F%2Faipo.oecd.org%2F2021-data-policyInitiatives-25416> accessed 13 October 2022.

'Federal Data Strategy'.[456] Against this background, the EU Data Act proposal and more broadly the whole EU Data Strategy seems to be rather unique, in that they lay the foundation of an ambitious set of rules concerning the use of data in different scenarios. The EU approach on data governance is strongly grounded on the idea of embedding EU values in it. It will certainly be interesting to keep monitoring the future global developments in this area and to observe whether, like in the case of the GDPR for data protection, also the Data Act could become a role model for data governance across the globe.

[456] OECD.AI Policy Observatory, Federal Data Strategy <https://oecd.ai/en/dashboards/policy-initiatives/http:%2F%2Faipo.oecd.org%2F2021-data-policyInitiatives-24303> accessed 13 October 2022.