KU LEUVEN CiTiP

CENTRE FOR IT & IP LAW

# CiTiP Working Paper Series

## White Paper on the Data Act Proposal

(Executive Summary)

**Edited by**

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

CiTiP Working Paper 2022

KU Leuven Centre for IT & IP Law - imec

26 October 2022

# 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.