Data Sharing Regulation in Europe

Edited by
Laura Zoboli and Maciej Bernatt

First published 2025

ISBN: 978-1-032-16371-0 (hbk)
ISBN: 978-1-032-16372-7 (pbk)
ISBN: 978-1-003-24825-5 (ebk)

Chapter 7

The Interplay of Data Protection, Competition Law, IP Law and Data Sharing

Laura Zoboli and Maciej Bernatt

DOI: 10.4324/9781003248255-11

The funder of the Open Access version of this chapter is University of Warsaw.

Routledge
Taylor & Francis Group
LONDON AND NEW YORK

7 The Interplay of Data Protection, Competition Law, IP Law and Data Sharing

Laura Zoboli and Maciej Bernatt

7.1 Introduction

The EU's commitment to promoting data sharing through legislative initiatives such as the Open Data Directive, the Data Governance Act, the Digital Services Act, the Digital Markets Act and the Data Act underscores the vital importance of creating an environment that supports data-driven innovation while upholding transparency, accountability and privacy. These regulatory efforts address challenges related to data access, interoperability and fairness, aiming to foster thriving and inclusive digital and data markets throughout Europe.

Despite these initiatives, a critical gap seems to persist in the realm of B2B data sharing. This book has highlighted how, despite its recognized potential to drive innovation and create value, B2B data sharing is subject to several legal limitations and – as seen in Chapter 1 remains limited – which significantly impacts the competitiveness and innovation potential of firms. The scarcity of B2B data-sharing initiatives underscores the need for focused attention and strategic interventions to unlock the full potential of data-driven collaboration among businesses.

By delving into the regulatory frameworks affecting B2B data sharing and revealing their lack of coherence, this book has provided valuable insights and actionable strategies for businesses, policymakers and other stakeholders. Navigating the complex landscape of data sharing in the digital age is no small feat, but understanding these dynamics is crucial for fostering collaboration, innovation and value creation.

As we conclude this exploration of B2B data sharing, we recognize the pivotal role it plays in shaping the future of the digital economy. By promoting collaboration and innovation, B2B data sharing has the potential to unlock new opportunities and drive societal progress. Thus, this book contributed to the discourse on aligning relevant regulatory frameworks and harnessing the full benefits of data-driven collaboration in the business world.

In this context, this conclusive chapter proceeds on two critical fronts that should be addressed to advance the public debate in the direction of contributing to an effective data-sharing system in the EU. First, general regulatory frameworks – specifically, competition law, intellectual property law and personal data protection law – impose limitations on the extent to which firms can share data. The following sections will explore the dynamics between these laws and consider how to

DOI: 10.4324/9781003248255-11

enhance the existing legal framework to better incentivize data sharing especially at the B2B level, while ensuring that values associated with competitive markets, innovation and privacy are duly protected in the data-sharing process. Second, the possible need for greater coherence among the new legislation adopted by the EU, which are designed to facilitate data sharing within the data economy and digital market. Data spaces are proposed as an intermediate solution that could harmonise horizontal and vertical regulatory frameworks, that aims to align with fundamental interests and rights while, at the same time promoting data sharing and, consequently, data-driven innovation.

7.2 IP, Competition and Personal Data Protection Laws as Limitations to Data Sharing

This section seeks to identify the limitations to data sharing imposed by intellectual property, competition and data protection laws. By focusing on how these regulatory frameworks may hinder or fail to incentivize data sharing, this section sets the stage for the subsequent section, which will explore the complementary aspects and consider how the same regulations can, under certain conditions, also facilitate data sharing. As framed in the following subsections, these three areas of law establish principles that can limit data sharing ("limiting principles"), which must be considered when interpreting new EU legal acts designed to promote data sharing within the EU internal market.

7.2.1 IP Perspective

While new pieces of EU legislation, discussed later, aim to facilitate data sharing, intellectual property law may sometimes contradict this objective. These limitations can be expressed in two dimensions: (i) the limited role of IPRs concerning data, which, as will be seen in section 3.1, primarily pertains to data collections; and (ii) the interference between IP protection and regulations promoting data sharing.

Regarding the first dimension, as discussed in detail in Chapter 6, IPRs can certainly be seen as a tool to reinforce the position of data holders, making it necessary to scrutinize the intersection between data assets and IPRs. However, patents and copyrights cannot protect data per se. For data to be covered by patent protection, it must exhibit factual-technical properties imparted by the patented process, making it suitable for patenting. Legal precedents clearly indicate that patent protection does not extend to data produced or generated from patented processes. Similarly, copyright cannot protect information generated through automated processes because it is not considered a product of intellectual creation, regardless of the intellectual effort invested in developing the technology that produces or processes the data. Consequently, data lacks the requisite level of originality required for copyright protection. Trade secret protection, however, retains its relevance in the context of data. The interpretation of trade secret requirements is already complex in traditional markets, and this complexity increases in the realm of data due to its multifaceted and often non-secret nature. This influences the assessment of the economic value of data and the adequacy of protection measures. This complexity is a

likely explanation as to why both the Data Governance Act and the Data Act focus primarily on the relationship between trade secrets and data-sharing obligations. The protectability of data under trade secret law depends on recognizing that data is not a homogeneous category. The distinction between raw data and processed data is particularly significant. Only processed data serve as carriers of informational capital, whereas raw data lack meaning until analyzed. Consequently, unprocessed data cannot constitute a trade secret because they do not convey information; digital encoding is necessary to imbue them with meaning. Conversely, "encoded" data can be subject to trade secret protection precisely because of the "informational" nature they acquire.

Regarding the second dimension, while new pieces of EU legislation aim to facilitate data sharing, IPRs can sometimes create obstacles. First, the DGA lacks specific indications on sharing data under IPR protection. It is clear, however, that DGA obligations apply only if compatible with international intellectual property agreements, such as the Berne Convention, the TRIPS Agreement and the WIPO Treaties. Second, to assess the interaction between IP and data sharing, the Data Act is crucial, particularly as it clarifies the scope of the Trade Secrets Directive. There certainly was a need for clarity on whether current exceptions adequately support data-driven and green economies and how these tools can combat illicit data acquisition, use and disclosure effectively and this – as it will be seen in section 5 below – has been addressed by the Data Act only in part.

7.2.2 Competition Law Perspective

Competition law may in certain circumstances impose limitations on the scope of permissible data sharing. Generally, since competition law aims at elimination of business practices which restrict competition, it makes such kinds of B2B (business-to-business) data-sharing illegal which would amount to restriction of competition. As explained in detail in Chapter 5, two principal scenarios in this respect can be mentioned.

First, within the ambit of Article 101 TFEU, data sharing is prohibited by competition law when it facilitates collusion between firms. This happens once data shared is in itself sensitive or can be used to infer information that is sensitive and in result facilitates the coordination of firms' behavior on the market. The Commission Horizontal Guidelines[1] explain, for example, that "aggregation of commercially sensitive information into a pricing tool offered by a single IT company to which various competitors have access could amount to horizontal collusion".[2] However, the exchange of raw data in itself will not be problematic. It is when data collected feeds in the sensitive information which is shared between firms when competition law prohibitions kick in. The background rationale is the

1 Communication from the Commission, *Guidelines on the applicability of Article 101 of the Treaty on the Functioning of the European Union to horizontal cooperation agreements* [2023] C(2023) 4752 final (hereinafter "Horizontal Guidelines"). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=oj:JOC_2023_259_R_0001

2 *Ibid*., para 402.

reduction of uncertainty among firms on the market with respect to the timing, scope and specifics of the conduct to be adopted in the market:[3] uncertainty is a key feature of competitive markets, and its reduction may have negative consequences for the ways in which markets operate.

Second, competition law limits data sharing once potential violation of Article 102 TFEU is at stake. In short, a dominant firm can be subject to antitrust investigation for forcing its business customers or individual consumers to share their respective business or personal data. The European Commission investigation in *Amazon Marketplace*[4] and the Bundeskartellamt investigation in *Meta* case[5] are illustrations here. The former case suggests that such practices should not be merely perceived from the exploitation perspective: accumulation of data by a firm that is already dominant may lead to further entrenchment of such a firm's position on the market by giving it advantage over its actual and potential competitors.

7.2.3 Personal Data Protection Perspective

The personal data protection regime in the EU imposes a broad and diverse set of limitations on data sharing. Indeed, the principal rationale behind personal data protection is to impose limits on how personal data can be processed and by doing so to safeguard fundamental rights, i.e. right to privacy. As explained in detail in Chapter 3, sharing of personal data is strictly restricted due to, among others, (i) broad, functional definition of personal data, which consequently also includes pseudonymized data; (ii) far-reaching protection of such personal data which are sensitive or concern children; (iii) strict requirement of freely given consent of data subject for processing of his or her data; (iv) purpose limitation (in principle personal data cannot be further processed in a way incompatible with the initial purpose); (v) data minimization rules (as a result of which only the necessary amount and category of data can be shared to achieve the purpose of data sharing). What's more, EU data-related laws tend to refer to GDPR to limit its scope of application (as it often also does for IPRs). On one hand, the Regulation on the free flow of non-personal data[6] states in Article 2(2) that where personal and non-personal data in a dataset are inextricably linked, the Regulation does not prejudice the application of GDPR. On the other hand, Article 7(8) of the DMA regulates the exchange of data between the gatekeeper and the provider of number-independent interpersonal communication services which makes a request for interoperability. It provides that only personal data of end users which are necessary to provide effective

3 See Mariateresa Maggiolino, Chapter 5.

4 European Commission, *Commission Decision of 20.12.2022 relating to a proceeding under Article 102 of the Treaty on the Functioning of the European Union (TFEU) and Article 54 of the EEA Agreement Cases AT.40462 – Amazon Marketplace and AT.40703 – Amazon Buy Box* [2022] (published 17 February 2023) C(2022) 9442 final.

5 Case C-252/21 *Meta Platforms and Others v Bundeskartellamt* [2023] EU:C:2023:537.

6 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 L303/59.

interoperability can be shared between these two entities, and only if such sharing is compliant with the GDPR. In this direction, Joanna Mazur argues in Chapter 3 that gatekeepers are likely to rely on the GDPR to deny the implementation of data-sharing obligations listed in the DMA.[7]

7.3 IP, Competition and Personal Data Protection Laws in Service Data-Sharing

This section aims to explore how intellectual property, competition and data protection laws can facilitate data sharing. By examining the potential of these regulatory frameworks to promote data sharing under certain conditions, it sets the stage for understanding how these laws can complement new EU legal acts designed to encourage data sharing within the EU internal market. As outlined in the following subsections, these three areas of law establish principles that, when interpreted and applied thoughtfully, can enhance data sharing while still protecting exclusivity, innovation, competition and privacy ("fostering principles").

7.3.1 IP Perspective

Reflecting the structure used to address the role of IP as an obstacle to B2B data sharing in section 2.1 above, this section considers IP as a potential facilitator in two dimensions: (i) the role of IPRs in the data realm and (ii) the interaction between the IP regulatory framework and regulations promoting data sharing.

Regarding the first dimension, the protection of databases or data collections is paramount. Collections of works receive explicit protection under international and European law. For example, Article 2 of the Berne Convention safeguards "collections of literary or artistic works, such as encyclopedias and anthologies, which, due to the selection and arrangement of their contents, constitute intellectual creations". This definition has expanded to include productions in literary, scientific or artistic fields, irrespective of their form of expression. The TRIPS Agreement and the WIPO Copyright Treaty reinforce this broader interpretation, specifically mentioning "compilations of data or other material", whether in machine-readable or other forms, as potentially eligible for protection if they exhibit creativity in selection and arrangement. In the EU, Directive 96/9/EC on the legal protection of databases adopts this approach, defining a database as "a collection of independent works, data, or other materials arranged systematically or methodically and individually accessible by electronic or other means". This directive mandates EU Member States to ensure copyright protection for databases resulting from an author's intellectual creation, establishing databases as distinct objects of copyright protection in Europe. However, concerns persist regarding databases' eligibility for copyright protection based on the requirement of "originality", initially designed for artistic creations. To address these challenges and foster information

7 See Joanna Mazur, Chapter 3.

technology development, Directive 96/9/EC introduces a two-tier system: copyright protection for 'original' databases and a sui generis database right for those that do not meet the minimum originality standard but result from significant investment. The first layer of protection – copyright for "creative" databases – is rare in practice, especially with the rise of big data, where databases often lack a specific approach or strategy, being products of purely technical considerations. This also affects the second layer – *sui generis* protection – as randomly collected "big data" may not meet the necessary investment level. For *sui generis* protection, legislation requires a "considerable human, technical, and financial" investment, focusing on qualitative and quantitative aspects. Notably, this protection does not extend to investments solely for creating data, as clarified in court judgments related to the unauthorized use of sports event calendars. Even when a database is awarded protection under copyright or the *sui generis* right, the object of protection remains only the "structure" of the database, referring to the selection or arrangement of the content. Both international treaties and European legislation are clear that protection "shall not extend to their contents" or "mere facts or data".

As per the second dimension, the key regulation to look at is the Data Act that impacts on both trade secret and *sui generis* protection in the data realm. It is true DA stipulates that data holders cannot refuse access requests solely on the grounds of trade secrecy. However, if third-party access involves trade secret-protected data, disclosure is contingent upon demonstrating that such disclosure is strictly necessary for the agreed-upon purpose between the user and the third party. In balancing these interests, the DA introduces exceptions to the trade secret holder's right to decide on access and use by third parties. It aims to increase data circulation while preserving the confidentiality of trade secrets and safeguarding their economic value. The DA requires data holders and users to adopt necessary measures to preserve data confidentiality before disclosure, such as through contractual terms, confidentiality agreements and technical standards. Amendments in subsequent versions of the DA provide additional exceptions and safeguards to better balance conflicting interests and protect trade secret holders. These amendments require trade secret holders to identify protected data and allow them discretion in decisions related to data sharing, especially where economic harm from disclosure is likely. In conclusion, while the Data Act facilitates greater openness to trade secret-protected data within defined parameters, it introduces complexities and uncertainties. These include ambiguities in regulatory language and challenges in harmonizing trade secret protection with data circulation imperatives. This detailed regulatory framework, while protective, may inadvertently hinder data circulation and potentially conflict with the inherently flexible nature of trade secret protection. Additionally, the DA impacts the *sui generis* database right provided by Directive 96/9/EC. Article 35 of the Data Act stipulates that the *sui generis* right does not apply to databases containing data obtained or generated from the use of a related product or service. This provision ensures that users' rights to access and use such data, as established in Articles 4 and 5 of the Data Act, are not hindered. While many see this provision as not introducing a novel element, as it could be inferred from Directive 96/9/EC, it addresses the digital economy's need for clarity

in facilitating data circulation and sharing, particularly by preventing data lock-in from user-generated data in the IoT ecosystem.

7.3.2 Competition Law Perspective

In section 2.2 competition law was considered to stay in the way of such data sharing which facilitates collusion and such use of data by a dominant firm that amounts to abuse of its dominant position. The former situation, which constitutes a 'by object' restriction of competition, must be distinguished from data sharing among competitors. While the latter may potentially restrict competition, it lacks the 'by object' characteristics and may qualify for either an individual exemption under Article 101(3) TFEU or one of the group exemptions provided in EU secondary law, such as exemptions for standardization or R&D agreements.[8] Data pools[9] are a key example here. In particular, data pool agreements under which undertakings licence specific datasets to a central administrator in order to fully exploit its whole value by means of big data analytics,[10] are likely to escape Article 101 TFEU prohibition[11] if data pool agreements are correctly built and abide by the participating undertakings.[12] In other words, data pools can facilitate data-sharing without raising substantive competition law related risks.

8 Please note that "by object" restrictions are unlikely to meet either individual or group exemption conditions.

9 A data pool is a data sharing system between companies, which involves an element of reciprocity, whereby at least some companies contribute data, *see* Martina Anzini, Anne-Carine Pierrat, 'Data Pools as Information Exchanges between Competitors: An Antitrust Perspective' (CEP 2020). Available at:: https://www.cep.eu/fileadmin/user_upload/cep.eu/Studien/cepInput_Data_pools/cepInput_Data_Pools_as_Information_Exchanges_between_Competitors_An_Antitrust_Perspective.pdf.

10 Oscar Borgogno, Giuseppe Colangelo, 'Data sharing and interoperability: Fostering Innovation and Competition through APIs' (2019) 35(5) Computer Law & Security Review.

11 If necessary measures are implemented, they cannot be classified as "by object" restrictions. The Horizontal Guidelines underline that "a data pool in which (partly) commercially sensitive data is exchanged which addresses information asymmetry in a non-concentrated market and that will result in benefits for consumers is unlikely to be considered as a restriction by object if the participants ensure that any commercially sensitive data that they exchange through the pool is necessary and proportionate to achieve the pro-competitive aim" (Sec 418). The Guidelines explain that participants can, for instance, rely as much as possible on aggregate and historical data, reduce the frequency of the exchange and implement measures to restrict access to the information exchanged and/or to control how it is used (ibid.). The participants should ensure that the arrangement is set up in a transparent manner (ibid.).

12 The 2023 Horizontal Guidelines explain that (i) participants in a reciprocal data-sharing arrangement such as a data pool should in principle only have access to their own information and the final, aggregated, information of other participants; (ii) technical and practical measures ensure that a participant is unable to obtain commercially sensitive information from other participants individually (Sec 408). In addition, the Guidelines encourage that (i) the management of a data pool can be assigned to a trustee that is subject to strict confidentiality rules as regards the information received from participants in the data pool; and (ii) undertakings that manage a data pool should also ensure that only information that is necessary for the implementation of the legitimate purpose of the data pool is collected (Sec 408).

Such a neutral scenario must be distinguished from situations where competition law (and, more recently, the DMA) actively promotes data sharing – namely, when access to data held by a dominant firm (or a gatekeeper, in the case of the DMA) is mandated or when fair terms for data access are ensured. Three approaches can be considered here. First, and most controversially, is to mandate access to the dominant firm's data by relying on the essential facility doctrine. A principle challenge which needs to be overcome by competition authority is to prove that access to the dominant firm's data is indeed indispensable and in particular that it cannot be accessed in different ways in an economically viable way (for example by means of its duplication).[13] Second, this approach aligns with the conditions set out in the *Slovak Telekom* ruling,[14] where access to a dominant player's data – while not denied in principle – would need to be mandated if the dominant firm's behavior is found to be contrary to this obligation, ensuring that access is granted under fair, non-discriminatory, and reasonable terms. The third approach, which is applicable in case of gatekeepers are various data-sharing obligations imposed by virtue of Article 6 and Article 7 DMA that will be considered more in detail in section 5 below. In particular, prohibitions applicable to gatekeepers, particularly Article 6(2), serve as an additional safeguard against the excessive use of other firms' or consumer data and play a complementary role vis-à-vis competition law. Last, one may consider that merger scrutiny can also play a role in preventing excessive market power, also in data-rich industries, to ensure that these consolidations do not lead to monopolistic control over vast amounts of data, which could stifle competition and innovation. In a nutshell, examining the potential impacts of mergers on market dynamics, regulatory bodies can also prevent the creation of data monopolies that could abuse their dominance, contributing to ensuring that data remains accessible and not overly concentrated in the hands of a few entities.

7.3.3 Personal Data Protection Perspective

While the regime of personal data protection is often perceived as a main obstacle for data sharing in the EU, the rules contained in GDPR offer a certain space for data sharing. First, the GDPR applies to personal data, and while it defines personal data very broadly, it does not impose limits on sharing of anonymized data and other kinds of data which are not personal (such as industrial data). Other, less restrictive legal regimes such as the Regulation on the free flow on non-personal data impose the rules under which such data is shared.

Second, the GDPR does not prohibit, as such, sharing of personal data by a data controller with third parties for commercial purposes. While in practice this is likely to be difficult, an interested data controller (a firm) should not rule out such a scenario completely. In this case such a firm should ask a data subject for consent[14] and offer a data subject an effective right to withdraw such a consent even

13 See more Maggiolino, Chapter 5.

14 Data sharing is in such a case a specific purpose within the meaning of Article 6(1)a of the GDPR. Such a consent would have to meet the criteria of being sufficiently specific and informed enough.

after his or her personal data was shared with third parties. The controller may also consider relying on grounds other than consent which are listed in Article 6 GDPR, for example a contract between data controller and data subject [Article 6(1)(b)].

Third, a potential for the GDPR compliant data sharing can be identified in the data-portability right contained in Article 20 of the GDPR. One can imagine that a data holder is approached by firms to encourage him or her to rely on his/her data-portability right to ask the data controller to share his/her data with such a firm or to upload such data directly to a platform used by such a firm.

7.4 Limiting and Fostering Principles of IP, Competition and Data Protection Laws

The analysis shows that IP, competition law and data protection law establish principles and rules that limit and foster data sharing that must be considered when creating a coherent data-sharing regime in the EU. Data sharing cannot occur in contravention of the interests these laws protect, namely the exclusivity and incentive of innovation via IPRs, competition and privacy. The table below illustrates these principles and confirms the need to balance them when creating a coherent data-sharing regime in the EU (Table 7.1).

Table 7.1 Limiting and Fostering Principles of Data Sharing

Regulatory Framework	*Limiting Principles*	*Fostering Principles*
Intellectual Property	• No copyright and patent on data, limiting the reinforcement of the data holders' position. • IPRs as a limit pro-data sharing regulation.	• (Residual) protection through trade secrets. • Copyright and *sui generis* right on databases. • Integration with the Data Act.
Competition Law	• Article 101 TFEU: risk of facilitating collusion via data sharing. • Article 102 TFEU: risk of imposition of data-sharing obligations by dominant firms.	• Article 101(3) TFEU: possible exemptions for data pooling and standardization or R&D agreements. • Integration with the Digital Markets Act. • Merger scrutiny can potentially contribute to preventing excessive data concentration.
Data Protection	• Data protection as a limit pro-data sharing regulation. • Broad, functional definition of personal data, with mixed datasets falling under GDPR. • Strict requirement for freely given consent for data use. • Purpose limitation and data minimization rules.	• Facilitation through anonymization. • Consent mechanism. • Data portability. • Increased trust in data sharing.

7.5 Coherence of EU Data Sharing Acquis

While intellectual property, competition law and data protection law may, in some respects, incentivize data sharing, a key role is to be played by pro-data-sharing regulations. Indeed, the EU has introduced a plethora of new regulations aimed at governing data access, transfer and sharing, creating a complex and often overlapping legal framework. This book has dissected this system, highlighting where these overlaps cause issues in coherence and legal certainty, and providing clarity on which rules firms should follow in various data-sharing scenarios. In other words, we can certainly talk today about an EU data-sharing acquis which aims to promote data sharing in the EU. However, the question remains whether these new legislation are coherent with one another and have the actual potential to stimulate data sharing in the EU. The following analysis intends to frame the pros and cons of the current scenario, trying to envisage paths for reflection on how to make it more conducive to pro-data sharing, especially among private entities.

As addressed in Chapters 2 and 4 of the book, the new EU legal framework covers B2B, G2B and B2G data sharing. It aims to stimulate data sharing by introducing a common EU regulatory framework, thus increasing legal certainty, rather than imposing a sharing obligation. Mandated data sharing is introduced only in specific circumstances where the EU legislator identifies either a specific market failure (e.g. in a specific sector, vis-à-vis gatekeepers, etc.) or a public interest reason, such as the B2G data-sharing obligation in the case of a public emergency, justifying direct intervention in market dynamics. Therefore, mandated data sharing is the exception, not the general rule, also within the new EU regulatory framework. More in detail, the 2019 Open Data Directive (ODD), replacing the Public Sector Information (PSI) Directive, introduces new rules to stimulate the sharing of data held by public authorities with the private sector, facilitating government-to-business (G2B) data sharing. The Data Governance Act (DGA) introduces a governance framework to stimulate both G2B and business-to-business (B2B) data sharing. Recently adopted, the Data Act introduces rules to stimulate B2B data sharing and to grant users' access to IoT generated data also in favor of third parties and data sharing from the private sector to the public sector in case of a public emergency, addressing also B2G data sharing. The Digital Market Act (DMA) includes specific data-sharing obligations, mandating digital gatekeepers to share their data with competitors under certain circumstances. It complements sector-specific rules that mandate data sharing in industries such as chemical, banking, automotive, electricity, telecom and postal services. Additionally, the right to data portability, as outlined in Article 20 of the General Data Protection Regulation (GDPR), allows data subjects to request the transfer of their personal data to a third party, resulting in B2B data sharing. In addition to the aforementioned regulations, there are sectoral regulations, such as the Directive on Payment Services (PSD2), which stipulates a right for third parties to access the banking data of consumers under certain circumstances.

Without attempting to cover all the discussions from Chapter 2 and Chapter 4 of the book, it is important to highlight some uncertainties regarding the relationship

between pro-data sharing regulations. Generally, the need to protect personal data, ensure exclusivity guaranteed by IPRs and prevent anti-competitive market distortion are external limits to these regulations and, in addition, what we can define as the EU data sharing acquis sometimes lacks internal coherence.

First, the Data Act (DA) makes significant strides in data sharing by setting up obligations to share data and a more general framework for data access and sharing. However, it fails to fully integrate with public sector information regulations like those in the Data Governance Act and the Open Data PSI Directive. Moreover, it does not sufficiently address issues such as manufacturers harvesting data from publicly purchased devices, leaving public procurement bodies to manage these concerns.

Second, the Data Governance Act (DGA) aims to facilitate the reuse of public sector data, including personal, confidential and IP-protected data, provided it respects existing rights. It establishes intermediaries for data-sharing facilities and data spaces but does not override third-party rights, requiring a methodology for resolving rights issues before granting access.

Third, the Digital Markets Act (DMA) focuses on gatekeepers (namely, undertaking providing core platform services designated pursuant to Article 3), imposing obligations to provide access and portability rights. However, it lacks a standalone right for business users to access and port data, potentially leading to litigation over inferred data. The DMA also mandates that advertisement repositories be accessible via APIs, with provisions for regulatory access for enforcement and research purposes. As is known, the DMA is part of the Digital Services Act Package together with the Digital Services Act, that applies to providers of intermediary services including online platforms.

Fourth, the Open Data Directive (ODD) governs access to public sector information for commercial use, creating a level playing field. Operating independently from the Data Act, it is limited by intellectual property rights and business confidentiality restrictions, focusing on public-good data.

Fifth, if it is true that general regulations related to the data realm – primarily the GDPR and the Regulation on the Free Flow of Non-Personal Data (FFD) – address the movement of personal and non-personal data within the EU internal market, at the same time they create obstacles to data sharing by requiring full compliance with their (sometimes) complex provisions and by prevailing on pro-data sharing provisions.

Lastly, considering one of the sectoral frameworks as an example, the PSD2 introduces specific rules for the payment services sector, including provisions for data access and transfer aimed at enhancing competition and innovation in financial services (Table 7.2).

In more general terms, firms may face uncertainties regarding which regulations apply in specific situations. The interplay between general and specific laws complicates compliance, particularly when specific rules do not provide clear guidance. For instance, if the DMA does not offer a coherent solution, businesses might turn to the general principles of the Data Act or other sector-specific laws. The DMA imposes obligations on gatekeepers to provide data access

Table 7.2 Data Sharing Regulations in the EU

Regulation	*Data Type*	*Pro-Sharing Objective*	*Main Tools*
DA	Private data.	Private data sharing.	Obligations to share data (B2C, B2B, B2G) + general framework for data access and sharing.
ODD/DGA	Public data.	Public data reuse ("as open as possible").	Obligation on Public Sector Bodies to offer public data for reuse (G2B).
DMA	Private data.	Private data access and portability.	Obligation on gatekeepers to provide access and portability rights.
GDPR	Personal data.	Free flow and data protection.	Framework for digital trust + portability + transfer, etc.
FFD	Non-personal data.	Free flow.	Ban on data localization measures.
Other	Various.	Sector-specific.	Sector-specific legislation (e.g. PSD2) and sectoral data spaces.

but does not specify which data is covered, potentially limiting business users' rights. Gatekeepers may also claim *sui generis* database rights, further restricting access. The DGS encourages the reuse of public sector data, but the ODD limits it to non-IP-protected data, while one can believe that public sector bodies must facilitate access while navigating intellectual property and confidentiality concerns.

Therefore, in order to improve the regulatory landscape, simplifying and harmonizing overlapping regulations can provide better legal certainty. In this direction, clearer integration of public sector information rules within the DA is needed. In addition, the DMA could be refined to explicitly grant access and portability rights to business users, not just end users. This would empower businesses to leverage data more effectively against gatekeepers. Establishing clearer guidelines for data intermediaries and data spaces can enhance data sharing. Ensuring that these entities cater to small businesses as well as large platforms is crucial for fostering innovation and competition. Moreover, developing frameworks that explicitly address the tensions with data protection, IP and competition law – as it is for example the case of DA and trade secrets – can be more conducive to a vibrant data economy.

7.6 Data Spaces as the Possible Place to Balance the Regulatory Frameworks

As discussed in various chapters of this book (2, 4 and 6), the EU is actively supporting the creation of Common European Data Spaces in strategic sectors to overcome technical, privacy and security barriers that currently hinder data sharing in specific industries. Announced in the 2020 Data Strategy, the European

Commission detailed these Common European Data Spaces further in a Staff Working Document published in February 2022 and the DGA and the DA contributed to define their structure. Each Data Space aims to create a single market for data, encouraging data sharing among firms in specific strategic sectors (e.g. healthcare, industrial manufacturing, agriculture, finance, mobility, the Green Deal, energy, public administration). The Commission will introduce common interoperability standards and sectoral data governance rules, such as model contracts, licenses and access rights, while the EU budget will fund the development of common IT infrastructures for each Data Space.

For the purposes of this chapter, data spaces can be viewed as an intermediate scenario where various EU regulatory frameworks converge to facilitate data sharing. These spaces can help balance the need to protect IPRs, personal data and competition while promoting data sharing in both B2B contexts and with public sector bodies. They also provide a platform to address the inconsistencies and lack of communication among existing EU pro-data sharing regulations. Additionally, it is essential to note that obstacles to data sharing are not only legal but also technical and cultural, and data spaces aim to overcome these by creating an interoperable and secure framework. EU data spaces aim to promote the availability of large pools of data in specific sectors and domains of public interest, combined with the technical tools and infrastructures necessary for data use and exchange, and appropriate governance mechanisms.

Despite being sector-specific, data spaces share common features. Even though only the health data space proposal has been released, insights into their governance mechanisms can be inferred from EU policy documents on data spaces in general.[15] Structurally, data spaces involve data relationships between trusted partners who adhere to high-level standards and guidelines related to data storage and sharing.[16] The goal is to accelerate digital transformation in identified fields by overcoming legal and technical barriers to voluntary data sharing and addressing trust issues through the development of fair, practical and clear rules for data use.[17] Data spaces aim to create an environment where market participants feel empowered to share more data for economic and societal use while retaining control over the data they generate. By making available large pools of good-quality and interoperable data in specific sectors, combined with the necessary infrastructure for data use and exchange, and appropriate governance mechanisms, data spaces should facilitate increased data movement across Member States and sectors.[18]

15 In addition to the policy documents, starting from 2021 the EU has launched a series of preparatory actions in the various sectors. *See*, for example, European Commission, 'Digital Europe Programme (DIGITAL) Call for proposals – Preparatory actions for Data Spaces' (2021). https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/digital/wp-call/2021/call-fiche_digital-2021-prepacts-ds-01_en.pdf

16 Gaia-X, 'What is a data space?', White Paper 1&2022, https://gaia-x-hub.de/wp-content/uploads/2023/11/GX-White-Paper-Data-Space.pdf (last accessed 30 January 2024).

17 European Commission, *Commission Staff Working Document on Common European Data Spaces* [2022] SWD(2022) 45 final 16.

18 Ibid., 21.

To address the crucial interoperability requirement, the Data Act allows the Commission to adopt guidelines specifying interoperability standards for the functioning of data spaces. This includes architectural models and technical standards implementing legal rules and arrangements fostering data sharing, such as access rights and technical translations of consent or permission.[19] Through Article 33 on data interoperability, the Data Act aims to contribute to developing common data spaces. However, the vagueness of some provisions in the Data Act risks hindering rather than promoting the creation of data spaces.[20] In particular, the Data Act makes no reference to interoperability across data spaces. It is crucial to specify whether the requirements for operators also apply to interoperability across sectors and how they align with each data space's features. Data spaces will rely on common technical infrastructures to facilitate coordination and ensure fair data pooling and sharing among actors.[21] Common elements across sectors will be implemented through a horizontal governance structure encompassing administrative and contractual rules that establish rights to access, process, use and share data transparently and reliably.[22] These common elements will be complemented by sector-specific rules.[23] According to the DGA, a European Data Innovation Board will be established to assist the Commission in developing data spaces, among other tasks.[24]

An important feature of data spaces is data control: data holders will control the data they generate and share, whether for payment or free.[25] Data owners can decide who accesses their data, for what purpose and under what conditions.[26] Increased trust will incentivize both businesses and individuals to share data, fostering an interconnected and competitive European data economy.[27] Moreover, data spaces should be open to organizations and individuals who respect EU rules and values.

19 European 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 Art 28(6).

20 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) SSRN Electronic Journal 81.

21 European Commission, *Commission Staff Working Document on Common European Data Spaces* SWD(2022) 45 final 4.

22 Johan Bodenkamp, 'Common European Data Spaces and The Data Economy' (Online Expert Seminar, 3 November 2022).

23 Governance frameworks must also comply with the relevant EU legislation (e.g. the GDPR, ePrivacy Directive, Platform to Business Regulation).

24 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 L152/1 Art 26. In particular they are commissioned to propose guidelines on data spaces and, more generally, to advise the Commission on security requirements, access procedures and cross-industry standards for data sharing.

25 European Commission, *Commission Staff Working Document on Common European Data Spaces* SWD(2022) 45 final 3.

26 Johan Bodenkamp, 'Common European Data Spaces and The Data Economy'.

27 European Commission, *Commission Staff Working Document on Common European Data Spaces* SWD(2022) 45 final 4.

This openness will foster competition among product and service providers requiring data sharing, avoiding potential competition lock-in due to manufacturers' specific protocols.[28] This is particularly relevant for the repair sector, where manufacturers often control data generated by their products, creating lock-in effects and hindering the market entry of after-sales service providers.[29]

For what is of specific interest in this chapter, data spaces are also crucial for ensuring compliance with European rules and cross-sectoral measures. They must operate fully within existing rules on personal data protection provided by the GDPR.[30] This means, for example, that health data can be processed for secondary use only for specific purposes established by the Regulation.[31] Data exchange must occur in a secure environment that guarantees adequate protection of personal data. Specific measures are established for sensitive data categories, where anonymization mechanisms can facilitate data sharing.

Additionally, data spaces must respect existing competition law and IP provisions. The Staff Working Document on Data Spaces states that data spaces shall comply with Articles 101 and 102 TFEU, the related Guidelines for Horizontal Cooperation Agreements,[32] and the Block Exemption Regulations.[33] Similarly, the Data Act ensures that its provisions do not prejudice the application of competition rules. However, neither the Staff Working Document on Data Spaces nor the Data Act thoroughly analyzes potential anti-competitive issues or measures to prevent collusion among competitors involved in data spaces. Regarding IPRs, data spaces – also thanks to data intermediaries – can balance the rights of IPR holders with the need for openness. For example, they can contribute to reconciling the data holders' interest in protecting trade secrets with the legitimate interests of users and third parties in accessing and using data. Indeed, data holders benefit from control over the data and the ability to determine trade secrecy prior to data sharing,

28 Ibid.

29 European 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 13.

30 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 (GDPR) [2016] OJ L119/1.

31 'Questions and Answers – EU Health: European Health Data Space (EHDS)' (*European Commission*, 3 May 2022) ec.europa.eu/commission/presscorner/detail/en/qanda_22_2712&gt (last accessed 30 January 2024).

32 European Commission, 'Communication from the Commission Guidelines on the applicability of Article 101 of the Treaty on the Functioning of the European Union to horizontal cooperation agreements' [2011] (2011/C 11/01) ("Horizontal Guidelines"). As is well-known, the Guidelines are intended to assist market participants in self-assessing whether an agreement restricts competition and, if so, whether it fulfills the criteria for an exemption. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52023XC0721(01)

33 Commission Regulation (EU) No 1218/2010 of 14 December 2010 on the application of Article 101(3) of the Treaty on the Functioning of the European Union to certain categories of specialisation agreements [2010] OJ L335/43 ("Specialisation Block Exemption Regulation"); and Commission Regulation (EU) No 1217/2010 of 14 December 2010 on the application of Article 101(3) of the Treaty on the Functioning of the European Union to certain categories of research and development agreements [2010] OJ L335/36 ("Research & Development Block Exemption Regulation").

which can lead to power asymmetries, and this poses a risk that data holders might preemptively determine data-sharing terms in a conflict of interest position.

Even if data spaces seem promising for resolving conflicts among regulatory frameworks, they might also fall short by requiring strict compliance or excessively relaxing critical rules, potentially facilitating competitor collusion. To truly support systematic data-driven innovation through increased sharing, these balancing acts should be integrated into the general regulatory framework, ensuring their relevance extends beyond specific industry-related initiatives.

7.7 Conclusions

The interplay of intellectual property IP law, competition law and personal data protection within the context of data sharing, particularly in the realm of B2B interactions, presents a multifaceted challenge that necessitates a balanced and nuanced approach. This chapter has provided a comprehensive examination of these intersecting legal domains, shedding light on both their limiting and facilitating roles in the pursuit of a robust data-sharing ecosystem. From the IP perspective, the tension between protecting proprietary data and promoting open access is palpable. IP laws, while essential for safeguarding innovation and rewarding creators, often create barriers to data sharing by restricting access to valuable datasets. This can stifle collaboration and limit the potential for new, data-driven innovations.

Competition law, designed to eliminate competition restrictive practices, can also act as a double-edged sword. On one hand, it aims to dismantle data silos and promote data accessibility; on the other, stringent regulations can inadvertently discourage data-sharing agreements that might be viewed as anti-competitive. Thus, striking a balance between fostering competition and facilitating cooperation is crucial. Personal data protection laws, epitomized by the GDPR in the EU, prioritize the privacy and security of individuals' data. While these laws are fundamental in building trust and ensuring ethical data use, they can complicate data sharing by imposing stringent compliance requirements. Businesses often find themselves navigating a complex legal landscape where the protection of personal data conflicts with the imperative to share and utilize data for innovation.

Conversely, these legal frameworks also provide pathways to support and enhance data sharing. IP law, through mechanisms such as licensing agreements and data pooling, can foster a collaborative environment where data is shared under agreed-upon terms that protect the interests of all parties involved. This promotes innovation while respecting intellectual property rights. Competition law, by advocating for open markets and dismantling anti-competitive practices, can create a level playing field that encourages data sharing. Policies that prevent data monopolies and promote interoperability are instrumental in ensuring that data flows freely and equitably among businesses, driving collective growth and innovation. Data protection laws, although stringent, offer a foundation for trust in the digital economy. By ensuring that personal data is handled responsibly, these laws build consumer confidence, which is essential for the widespread adoption of data-sharing

practices. Additionally, frameworks such as the GDPR encourage the development of privacy-preserving technologies, which can facilitate secure and compliant data sharing.

The coherence of the EU's data-sharing acquis remains a critical issue. The plethora of legislative initiatives – ranging from the Open Data Directive to the Data Act – reflects the EU's commitment to a thriving data economy. However, the challenge lies in harmonizing these frameworks to create a seamless regulatory environment. Inconsistencies and overlaps among these laws can create confusion and hinder the effective implementation of data-sharing strategies.

The concept of data spaces emerges as a promising solution to the regulatory complexities of data sharing. By creating structured environments where data can be shared under clear and consistent rules, data spaces can harmonize the various legal frameworks and facilitate cooperation. These spaces aim to balance the protection of fundamental rights and interests with the promotion of data-driven innovation, thereby providing a practical pathway to achieving the EU's data economy objectives. However, while data spaces show promise in resolving conflicts among regulatory frameworks, they may also prove inadequate by imposing overly strict compliance or excessively relaxing critical rules, potentially facilitating competitor collusion. To genuinely support systematic data-driven innovation through enhanced sharing, these balancing acts should be integrated into the broader regulatory framework, ensuring their relevance extends beyond sector-specific initiatives. In other words, it is crucial to recognize that while data spaces are important, we cannot invest everything in them alone; instead, we must strive for a harmonious and collaborative regulatory scenario.

In doing so, it is worth examining experiences beyond the EU system, such as those in India, the United Kingdom and Poland since they reveal diverse approaches to establishing nationwide data sharing schemes.[34] Typically, these efforts involve a central body tasked with approving datasets, managing data-sharing requests and arbitrating disputes among custodians and processors. While this centralized model offers security by allowing state oversight, it can strain under increasing data volumes and hinder cross-border initiatives within the EU. India's exploration of decentralized data custodians and blockchain verification represents an alternative approach. Empowering data subjects to control anonymization of their personal data further exemplifies India's progressive stance, surpassing even the stringent standards of the EU's GDPR. Meanwhile, the data trust model, extensively explored in India, Poland and the UK, presents an attractive regulatory alternative. Yet, it risks tech giants like Google and Facebook influencing data ethics and standards. Even with the adoption of data trust models, as observed in the UK, effective data

34 *See* Marcin Z Zieliński, 'Non-Personal Data Sharing Initiatives. A Comparative Approach' (2023). Available at: https://cars.wz.uw.edu.pl/images/konferencje/konferencje_miedzynarodowe/DATA%20SHARING/Non-personal%20data%20sharing%20initiatives.%20A%20comparative%20approach.pdf.

sharing demands robust legal frameworks like contracts, equitable trusts, corporate structures or regulatory oversight. Such frameworks often necessitate significant legislative intervention to be implemented effectively. Poland's innovative concept of placing unprocessed raw data in the public domain, thus bypassing legal protections, could bolster data-sharing popularity. However, reluctance from major data producers may hinder widespread adoption of this approach.

Moving back to the EU dimension, it is clear that the future of B2B data sharing in the internal market hinges on the ability that the EU institutions will have to navigate and reconcile the intricate interplay of IP, competition and data protection laws. By fostering an environment where these legal frameworks complement rather than conflict with each other, we can unlock the full potential of data-driven innovation. This chapter underscores the need for ongoing dialogue and strategic alignment among businesses, policymakers and other stakeholders to create a coherent and supportive regulatory landscape.

In conclusion, the journey toward an effective and inclusive data-sharing ecosystem is complex but attainable. By leveraging the strengths of IP, competition and data protection laws, and by exploring innovative solutions such as data spaces, we can pave the way for a vibrant digital economy that benefits all. This chapter contributes to the broader discourse on aligning regulatory frameworks, ultimately aiming to harness the transformative power of data for societal progress and economic growth.