Chapter 5
Legal Aspects of IDS: Data Sovereignty—What Does It Imply?

Alexander Duisberg

Abstract The claim of data sovereignty is inherently linked to putting the legal instruments and tools in the hands of each participant in the ecosystem, allowing freedom of contract as well as ensuring that exercising data exchange and consorted data usage in the data economy is in compliance with general and specific regulations, ranging from anti-trust to GDPR and cyber-security regulations as well as sector specific regulations. The IDS provides a framework and a technology to allow the parties to limit their transaction costs and to ensure effective enforcement through the concept of usage control. In a future world, this will include increased automation of contract execution (conclusion, performance, and enforcement), whereas the steps to reach that goal are plentiful and, as of now, still require to "set the scene" with the means of the traditional contractual agreements. This article provides an overview and orientation on the key legal areas and aspects to consider for stakeholders, participants, and the business more generally and in the application of the IDS architecture.

5.1 Data Sovereignty: Freedom of Contract and Regulation

The claim to success for the IDS is driven by the combination of a common framework of values and reliability, including the reference architecture, connector technology, certification, and an ecosystem that any and all contributors and participants can trust, in order to share and exploit personal and non-personal data within a multitude of sectors and appliances.

At its heart, IDS intends to facilitate and enable the freedom of research, development, and business by sharing and using data between different players *and* giving any contributor of data the opportunity to manage and maintain control over the data that it puts at the disposal of others.

A. Duisberg (✉)
Bird & Bird LLP, Munich, Germany
e-mail: Alexander.Duisberg@twobirds.com

B. Otto et al. (eds.), *Designing Data Spaces*,
https://doi.org/10.1007/978-3-030-93975-5_5

The claim of data sovereignty is inherently linked to putting the legal instruments and tools in the hands of each participant in the ecosystem, allowing freedom of contract as well as ensuring that exercising data exchange and consorted data usage in the data economy is in compliance with general and specific regulations, ranging from anti-trust to GDPR and cybersecurity regulations as well as sector-specific regulations. The following intends to provide an overview and orientation on the key areas to consider for stakeholders, participants, and the business more generally.

5.1.1 No Ownership or Exclusivity Rights in Data

Whereas the initial discussion about "who owns the data" dominated the initial phase of the data economy, policy makers, practitioners, and academics have now achieved an—close to unanimous—understanding that the defining and allotting "ownership" or other forms of exclusivity rights in data per se will not facilitate the development of the data economy. As a result of extensive consultation and debate, the focus has shifted to considering the issue of access and re-utilization of data as key to foster sharing and exchange of data, in order to unleash the potential of innovation through data, both in the private and the public sector.[1] While the outcome might appear "counter-intuitive" to some participants ("How can I not own 'my data'?"), it is clear that it cannot be up to legislation or government to take decisions which could favor one side of the market and ecosystem, for example, the "data producer" or the "data holder" or the "data processor" or the "data aggregator," etc. It is a grown consensus that while any unilateral determination of "ownership rights" in data would be premature while entering into and exploring the potential of largely unknown territories of the data economy, it appears quite likely to prevent rather than facilitate innovation through data.

As a result, the means and tools of enabling the data economy are based in contract law, i.e., regulation of data rights *inter partes* rather than *erga omnes*. The success of data sharing in the data economy depends on proper mechanisms of enforcing the contractual rights throughout the ecosystem.

By putting sample contracts at the disposal of all participants of the ecosystem, IDS gives orientation as well as the freedom to create contracts of their own that data providers, data brokers, and data consumers and any other participants can construe and implement their models for sharing data through licensing agreements of all sorts and kinds, without being prescriptive as to the kind and nature of the contractual relations.[2]

[1] EU Commission (19 February 2020) A European strategy for data. https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf. Accessed 28 January 2021; and Recitals of Regulation (EU) 2018/1807 on a framework for the free flow of non-personal data in the European Union (Free Flow of Non-Personal Data Regulation)

[2] See further details on the different kinds of data licensing agreements under Sect. 5.2.2.1.

5.1.2 Usage Control: Legally and Technically

Based on the concept of data licensing contracts that stipulate data usage rights under respective contract terms, the concept of IDS is to provide a technical solution which enforces such usage rights. The objective of IDS is to add to every dataset the respective protocols that define which data users ("data consumers") are authorized and shall be technically enabled to access the data that a data provider and/or data broker wishes to share with them, under which purposes and for which duration. That may include whether a user may extract, develop, combine, and further enhance such data, as well as onward-share the data and/or any derivatives of such data and related database, next to the dealing with what shall happen after such usage rights have ended.

In other words, IDS has the overall objective of usage control by combining organizational elements under the auspices of freedom of contract with a technical solution. That said, it does not (yet) have the aim of providing a fully automated technical implementation of all contractual parameters as an executable in binary form (comparable to the concept of smart contracts in the blockchain/distributed ledger technology).[3] In fact, the path toward parameterizing different types of contracts and ascertaining related contractual remedies under a governing law (to be selected) bears a multitude of complexities, which need to be further explored. The current effort of the "Legal TestBed" initiated by the "Plattform Industrie 4.0"[4] is a first important step in that direction. By nature of how the formation and interpretation of contracts work, it is not a trivial task and, hence, important to manage expectations what semi-automated contracting and contract enforcement can achieve.[5] Yet, the vision of IDS is right and the implementation requires a legal framework that includes and supports the implementation of technical usage control. With that, usage control will have a stronger effect than the traditional licensing models.

[3] For legal implications of the blockchain in Industrie 4.0 context, reference is made to the publication of the Working Group 4 of the Plattform Industrie 4.0 Blockchain and the Law in the Context of Industrie 4.0, available at https://www.plattform-i40.de/PI40/Redaktion/EN/Downloads/Publikation/blockchain-and-the-law-industrie4.0.pdf?__blob=publicationFile&v=6. Accessed 28 January 2021.

[4] The initiative "Legal TestBed" works on developing a digital testbed to investigate automated business processes and aims to provide policy makers and companies with recommendations for action concerning new legal standards. See further information on the initiative at https://legaltestbed.org/en/start/. Accessed 28 January 2021.

[5] Reference is made to the project and activities of the Working Group "Legal TestBed," which is working on a limited, automated contract negotiation and formation project, and further information available at https://www.plattform-i40.de/PI40/Redaktion/DE/Kurzmeldungen/2020/2020-10-06-rethinking-law.html (only available in German) and https://legaltestbed.org/en/the-testbed/. Accessed 28 January 2021.

5.1.3 Database Rights

Under current law, the most notable (yet largely unknown and underestimated) legal instrument available and applied to collections of data is the right of the database maker, as provided under the EU Database Directive 96/9/EC and implemented in each EU Member State.[6] The database right protects the investment into the systematical and methodical order of a collection of data in order to prevent extraction and/or re-utilization of the whole or a substantial part of the contents of the database,[7] but not the data as such.[8] That said, the database rights provide an important tool in managing data collections, which needs to be considered much more thoroughly in the context of the data economy. The database rights are limited to rightholders (including enterprises) who are nationals or have their habitual residence in the EU, and are construed as a sui generis right, giving the investor exclusivity rights for a duration of 15 years. It includes that the rightholder may transfer, assign, or grant usage rights under a contractual license; it applies independently of whether the actual content or the database as such is (also) eligible to copyright protection.[9,10] It is important to note that the holder of database rights does not enjoy absolute protection, but may only claim a breach of his rights where he has "made available to the public" if a lawful user extracts or re-utilizes other than insubstantial parts of its contents.[11]

Also, any substantial change to the existing database (e.g., made by a lawful user) may result in the creation of a fresh sui generis right in such new database.[12] EU Member States may also define certain usage rights, as permitted exceptions to the sui generis right, such as data extraction for private purposes, teaching, and scientific research, as well as extraction and/or re-utilization for public security or administrative or court procedures.

In essence, any provider of structured data should examine whether he/she can claim the database rights. If so, the rightholder should consider all options for granting licenses in the database as well as safeguarding his/her legal position against unwanted modifications and alterations, which could result in the creation of new sui generis rights.[13]

---

[6] E.g., Sections 87 lit. a–e German Copyright Act

[7] See Art. 7 para. 1 EU Database Directive.

[8] See Rec. (48) EU Database Directive, cf. "whereas the provisions of this Directive are without prejudice to data protection legislation" and *Rezlauf*, Holistic Approach to Handling Big Datasets Including Personal Data for EU-Companies, CRi 2020, 69.

[9] See Art. 7 para. 4 EU Database Directive.

[10] For example, a digital music file is a data collection (of bits and bytes) that enjoys copyright protection, whereas a data collection of sensor data retrieved from a machine does not.

[11] See Art. 8 para. 1 EU Database Directive.

[12] See Art. 10 para. 3 EU Database Directive.

[13] The sample contracts of IDS cater for this situation.

Notably, the EU Commission has envisioned as part of its EU Data Strategy to possibly revisit the EU Database Directive, in order to further enhance data access and use (see Sect. 5.1.6).[14]

5.1.4 Trade Secrets

Confidentiality agreements are generally a viable tool to protect confidential information. But how and what do you keep secret if you share data? What seems an oxymoron by nature needs to be carefully considered in any kind of data transactions.

When sharing data, it is not in first place the information that a data provider shares. It is rather the data provider who intentionally enables the data consumer (or a variety of them) and other participants in the ecosystem to derive and/or generate, each individually, new and different information and value from using the data. In other words, it is important to understand that the data provider cannot necessarily maintain control over what a data consumer makes out of the data that he/she provides.

When further looking into the information models of IDS,[15] the data provider does have certain control over the metadata that he/she shares and, thus, can define or limit the scope of possible conclusions that a data consumer can draw on the data provider's sensitive business information.

To give a practical example, the owner of a steel mill that shares runtime data of his/her machines in real time is providing considerable transparency about his/her current level of bandwidth and manufacturing capacity at any given point in time. He/she will want to avoid that this information is disclosed to his/her competitors and/or intermediaries who might use the information to influence market pricing. The factory owner who is interested in sharing data with a supplier of predictive maintenance services for his/her steel mill may want to (1) enter into confidentiality agreements as well as (2) select and limit the type of metadata that he/she shares with the service provider and certain intermediaries. When going further in sharing data with a business innovator working on an AI-based optimization of the manufacturing process, he/she may want to limit the data he/she shares to other parts of the metadata, in respect of the same manufacturing process.

[14] See p. 13 EU Commission (19 February 2020) A European strategy for data.

[15] The primary purpose of the information model as part of the IDS Reference Architecture is to enable (semi-)automated exchange of digital resources within a trusted ecosystem of distributed parties, while preserving data sovereignty of data owners. Once the relevant resources are identified, they can be exchanged and consumed via semantically annotated, easily discoverable services (see Section 3.4 of the IDS Reference Architecture Model 3.0, available at https://www.internationaldataspaces.org/wp-content/uploads/2019/03/IDS-Reference-Architecture-Model-3.0.pdf. Accessed 28 January 2021).

In addition to the tools of usage control and confidentiality agreements, however, it is important to consider the scope and inherent limitations under the EU Trade Secrets Directive (EU) 2016/943 and its varying implementation into national law of the EU Member States.

In essence, a data provider can claim trade secret protection for "*information*... which...is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to personal with the circles that normally deal with the kind of information in question...and *has commercial value because it is secret*...and has been *subject to reasonable steps*...*to keep it secret*."[16] While this test can exclude trade secret protection for data with no information value, it is clear that the commercial value is likely to lie in the related metadata. A data provider must therefore determine (and document internally) *before* sharing it whether certain data has commercial value *because* it is secret and which protective measures the data provider has taken to keep it secret (such as limited access internally on a need to know basis, technical security measures, etc.). Subsequently, the data provider will be in a position to define access rights for the data, subject to confidentiality agreements with data consumers, data brokers, and others, and which must be combined with a reliable technical and organizational framework in order to prevent unauthorized third-party access so that the trade secret protection extends when sharing the data.

The benefits of trade secret protection in shared data are obvious, as the trade secret owner has actionable rights to request cease and desist against unlawful data usage (i.e., without the trade secret owner's consent), claim damages against misappropriation of trade secrets, etc.[17]

5.1.5 Competition Law

Competition law in the digital world raises the most complex and currently uncertain issues to be solved.[18] The traditional tools of merger control have been expanded over the last few years, in order to capture and regulate scenarios where the market

[16] Art. 2 para. 1 lit. a–c EU Trade Secrets Directive; italics by the author

[17] See Art. 4 and 6 EU Trade Secrets Directive and its national implementations, e.g., Sections 6–8 German Trade Secrets Act.

[18] On December 15, 2020, the EU Commission has proposed the regulation on contestable and fair markets in the digital sector (Digital Markets Act) (https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020PC0842&from=de). Article 12 Digital Markets Act sets out an obligation to provide information on concentrations for the undertakings within the meaning of the Digital Markets Act. Also, the German legislator reformed the German Act Against Restraints of Competition (ARC). Largely this amendment entered into force on January 19, 2021. In future, mergers will only be subject to control if, among other things, one of the companies involved has an annual turnover in Germany of at least EUR 50 million, instead of the previous EUR 25 million, and in addition, another company involved has an annual turnover in Germany of at least EUR 17.5 million, instead of the previous EUR 5 million.

impact is less influenced by the mere size of the merging companies, but rather to also address situations where the focus of the contemplated transaction is on a data-rich target company with limited economic size considered by the traditional parameter.[19] Further, the investigations conducted by the German Federal Cartel Office against Facebook, in which it looked at the terms of use to capture a scenario of (allegedly) excessive data collection, give an indication on how authorities are trying to expand their reach in regard to the control of market dominant positions that rely on the accumulation of vast amounts of data and related data-driven business models.[20] Ultimately, the EU Commission has addressed in its EU Data Strategy the issue of imbalance in market power in relation to data-rich businesses ("data advantage"), putting on the agenda the need to define new ways of preventing market distortion and lack of competition,[21] leading in particular to the new EU Digital Markets Act.[22]

In its decision of February 6, 2019, based on Sec. 19 para. 1 ARC, the German Federal Cartel Office prohibited Facebook from, inter alia, using conditions that make the use of the eponymous social network Facebook by private users resident in Germany dependent on Facebook being able to link and use user- and device-related data collected during the use of the group's own services such as WhatsApp with the user accounts maintained for Facebook.com without the consent of the users. However, with decision of August 26, 2019 (VI-Kart 1/19 (V)), as a provisional order, the Higher Regional Court of Cologne found that even in the case of an assumed data protection infringement, Facebook had not abused its market-dominating position within the meaning of Sec. 19 para. 1 ARC. Hence, the Higher Regional Court Düsseldorf had ordered the suspensive effect of the appeal at Facebook's request. At the request of the German Federal Cartel Office, the Cartel Senate of the Federal Court of Justice reversed this order in a decision of June 23, 2020 (BGH, 23 June 2020—KVR 69/19), and rejected Facebook's application for an order of suspensive effect of the appeal.

[19] According to the explanatory memorandum to the 9th amendment of the ARC 2017 regarding Sec. 18 para. 3a ARC, the market position of an undertaking can also be significantly influenced by its access to data; see BT-Drs. 18/10207.

[20] It would exceed the scope of this contribution to discuss in detail the implications of this decision and the pending appeal procedures. But among the various questions to debate, one also needs to consider to which extent anti-trust authorities have the authority to assess the validity of GDPR compliance in such context (see the decision of the German Federal Cartel Office (https://www.bundeskartellamt.de/SharedDocs/Entscheidung/DE/Entscheidungen/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=8. Accessed 28 January 2021), and the decisions of the OLG Düsseldorf, August 26, 2019—VI-Kart 1/19 (V), and of the German Federal High Court of Justice, June 23, 2020 – KVR 69/19. Also see the review by *Haus* and *Cesarano*, Mehr-Daten für Facebook, NZKart 2019, 637 and the remark of the last-named decision by *Mohr*, LMK 2020, 432972.

[21] "Progress will need to be made together on the following issues: A case in point comes from large online platforms, where a small number of players may accumulate large amounts of data, gathering important insights and competitive advantages from the richness and variety of the data they hold. This can affect, in turn, the contestability of markets in specific cases—not only the market for such platform services, but also the various specific markets for goods and services served by the platform, in particular if the platform is itself active on such related markets." See p. 8 EU Commission (19 February 2020) A European strategy for data.

[22] See Sect. 5.3.2 with some further explanations on the EU Digital Markets Act.

Where companies exchange sensitive or confidential information relating to their market position (e.g., price information, but also other information that might allow coordinated behavior), each party must ensure—and assumes proper responsibility—not to restrict competition and/or distort markets through agreements restraining competition or resulting in coordinated behavior.[23] While exchanging, for example, sensor data through IDS is per se unlikely to result in direct coordination over pricing between competitors, or other restraints and anti-competitive practices (both at a horizontal level between direct competitors, and vertically between the different levels in a chain of distributing products and services in a given market), it is clear that each participant in a bilateral or consorted exchange of *data* assumes responsibility and must ensure to comply with applicable competition law. Accordingly, data providers, data brokers, and data consumers may need to limit the exchange of *market relevant information*, which is contained in or could be directly derived from exchanging "raw data" together with relevant metadata.

As a further consequence, the operator of a data space will want to safeguard in its information notices and terms of use that each participant to a data exchange is properly aware and undertakes to avoid exchanging market-sensitive information that could be abused and/or that could result in coordinated behavior.

5.1.6 EU Strategy on Data: The Relevance of Data Spaces

The EU Commission has set important milestones for transforming the single market into a digitally enabled market and making the EU "leading in a data-driven society" and empowering "people, businesses and organisations . . . to make better decisions based on insights from non-personal data, which should be available to all"[24] and creating a "data-agile economy."[25] Together with this ambitious claim, the EU Commission has presented its EU Data Strategy as a cornerstone to a wider framework of existing and upcoming regulation.[26]

The EU Data Strategy envisions three fundamental objectives, namely, (1) the free flow of data within the EU and across sectors; (2) full respect of European rules and values, including in particular personal data protection, consumer protection, and competition law; and (3) fair, practical, and clear rules for fair access and use of data, based on trustworthy data governance mechanisms.[27]

The EU Commission envisions new legislative measures to support those objectives, including in particular: (1) a cross-sectoral governance framework for data

[23] See Art 101–109 Treat of the Functioning of the European Union TFEU.

[24] See p.1 and 4 EU Commission (February 19, 2020) A European strategy for data.

[25] Ibid p.8

[26] EU Commission (19 February 2020) A European strategy for data

[27] Ibid. p. 5

access and use, (2) making available more high-quality public sector data for re-use, (3) a data act for horizontal data sharing across sectors, which may include revisiting the EU Database Directive and the EU Trade Secrets Directive, in order to facilitate and enhance access and (re-)use of data.[28]

Most notably, the EU Commission recognizes and endorses the fundamental importance of data spaces as part of the first pillar (1), aiming to "enable a legislative framework of the governance of common European data spaces,"[29] as well as providing significant investment and funding in High Impact Projects on European data spaces and federated cloud infrastructures.[30] It is clear by the wording and further considerations of the EU Commission that IDS and its key elements (i.e., the connector technology, reference architecture, usage control, certification scheme, and model contracts) provide the lead image and stand at the heart of this particular part of the EU Data Strategy. The EU Commission emphasizes that such data spaces shall "overcome legal and technical barriers to data sharing across organisations, by combining the necessary tools and infrastructures and addressing issues of trust, for example by way of common rules developed for the space. The spaces will include; (i) the deployment of data-sharing tools and platforms; (ii) the creation of data governance frameworks; (iii) improving the availability, quality and interoperability of data—both in domain-specific settings and across sectors."[31] The EU Commission has defined as a key action point to that end combined investments in the range of EUR 4–6 billion including direct investments of up to EUR 2 billion.[32]

As part of its data space strategy, the EU Commission has identified the following sectors where it intends to create "Common European data spaces": industrial/manufacturing, Green Deal, mobility, health, financial, energy, agriculture, public administration, and skills.[33] In other words, IDS represents a role model, if not a blueprint, for these sectors to prepare and develop—in an active dialogue with the relevant stakeholders—the related data space implementations in accordance with the EU Data Strategy.

[28] Ibid. p. 11 et seq.

[29] Ibid. p. 12 and 16

[30] To this Gaia-X, which is a project with representatives from politics, business, and science creating secure, federated European system that meets the highest standards of digital sovereignty while promoting innovation (see https://www.bmwi.de/Redaktion/EN/Dossier/gaia-x.html. Accessed 28 January 2021), is a constituent element that has further materialized since the EU Commission set out its Data Strategy in February 2020 (see p. 18 EU Commission (19 February 2020) A European strategy for data).

[31] See p. 16 et seq. EU Commission (19 February 2020) A European strategy for data.

[32] Ibid. p. 19

[33] Ibid. p. 22 et. seq. and its Appendix with further details

5.1.7 Data Governance Act: First Comments

The Data Governance Act of May 30, 2022,[34] is a pillar in the EU Data Strategy and will be complemented by the European Data Act to foster data sharing among businesses, and between business and governments,[35] and stands next to the Digital Markets Act[36] and the Digital Services Act.[37] It contains key elements of regulation for operators of data spaces.

Its principal areas of regulation cover the following objectives: (1) making public sector data available for re-use in situations where such data is subject to rights of others (such as privacy rights, IP rights, trade secrets, or other commercially sensitive information); (2) sharing data among businesses, against remuneration in any form; (3) allowing personal data to be used with the help of a personal data sharing intermediary that safeguards data subjects' rights under the GDPR; and (4) allowing data use on altruistic grounds.[38] As regards public sector data, the Data Governance Act complements and stands in addition to the Open Data Directive.[39] The overall objective is to "facilitate data sharing by reinforcing trust in data intermediaries,"[40] which are expected to play a significant role in data spaces, whereas the rules on access and use of data shall be covered by the Data Act.[41] The Data Governance Act defines as overall requirements that data should be "findeable, accessible, interoperable and re-usable."[42]

The Data Governance Act accentuates the role and provides notification obligations for providers of data sharing services ("data intermediaries"), in an approach to create a European model for data sharing of personal and non-personal data through "neutral data intermediaries," as an alternative to the current prevalence and market

[34] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance (Data Governance Act), OJ L 152/1 of June 3, 2022. Accessed 13 June 2022. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0767&from=EN. Accessed 28 January 2021

[35] See EU Commission press release: Commission proposes measures to boost data sharing and support European data spaces https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_20_2102/IP_20_2102_EN.pdf. Accessed 10 February 2021.

[36] Proposal Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0842&from=de. Accessed 10 February 2021

[37] Proposal for a Regulation on a Single Market For Digital Services (Digital Services Act) https://eur-lex.europa.eu/legal-content/de/TXT/?qid=1608117147218&uri=COM%3A2020%3A825%3AFIN. Accessed 10 February 2021

[38] Ibid. p.1

[39] EU Directive (EU) 2019/1024 on open data and the re-use of public sector information (Open Data Directive); Rec. (5)-(14) of the Open Data Directive and p.1 EU Commission (25 November 2020) Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act)

[40] p.1 EU Commission (25 November 2020) Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act)

[41] Ibid.

[42] Ibid.

power of integrated tech platforms that are commonly run by corporate businesses.[43] While this approach emphasizes the importance of data held in the public sector and ensuring data sharing across Member States,[44] it is by no means limited to the same.

A key requirement to safeguard trust and control over the data sharing between data holders and data consumers is ensuring the neutrality of the data intermediary. That implies that the data intermediary only acts as an intermediary in data transactions and does not use the data for other purposes.[45] The data intermediary shall have an establishment in the EU, or an appointed representative if offering the intermediary services from outside, and must follow a notification procedure (yet to be developed in the Member States) such that it notifies the competent registry/authority of its intention to provide intermediary services. In essence, the focus on data intermediaries accentuates the role and responsibility of operators of data spaces.

With regard to scientific research, for example, in relation to the health sector or environmental issues under the Green Deal, the Data Governance Act defines the role of "Data Altruism Organisations recognized in the Union," which are subject to a voluntary registration regime.[46]

From an institutional perspective, the Data Governance Act will create a "European Data Innovation Board," consisting of representatives of the Member States, the EU Commission, and representatives of relevant data spaces and specific sectors (e.g., health, agriculture, transport, and statistics).[47] It shall coordinate national processes and policies and support cross-sector data use within the "European Interoperability Framework" (EIF).[48]

As for data held by the public sector, the Data Governance Act establishes a few key principles: generally, public sector bodies shall not enter into exclusive agreements for the re-use of data they hold, nor may they restrict the availability of the data for re-use, unless (as an exception to the rule) where a data consumer receives exclusive rights for a maximum of 3 years, in order to provide a service or product in the general interest and under a national concession issued in accordance with general transparency principles.[49] In all other cases, public sector bodies shall grant rights to re-use public sector data based on the rules of transparency, equal treatment, and non-discrimination on grounds of nationality. The actual conditions for re-use must be proportionate and objectively justified with regard to categories of

[43] Ibid. p.6

[44] See Art. 3–8 Data Governance Act.

[45] Rec. (26) and Art. 11 para. 2 Data Governance Act

[46] Art. 1 para. 1 lit. c and Art. 17 Data Governance Act

[47] Rec. (40) Data Governance Act

[48] Rec. (41) Data Governance Act, see https://joinup.ec.europa.eu/collection/connecting-europe-facility-cef/about and https://joinup.ec.europa.eu/site/core_vocabularies/Core_Vocabularies_user_handbook/ISA%20Hanbook%20for%20using%20Core%20Vocabularies.pdf for examples of standards and specifications used by the European Data Innovation Board.

[49] Art. 4 para. 1–3 Data Governance Act

data and purposes of re-use and may define (among others) obligations in regard to secure processing environments provided and controlled by the public sector.[50] Transfers of highly sensitive non-personal data to third countries may be restricted by national Member States laws.[51]

The Data Governance Act requires data intermediaries to follow a notification procedure in regard to the following types of intermediation services: (1) between data holders (as legal persons) and data consumers both in bilateral or multilateral data exchanges, or the creation of platforms or databases that enable the exchange or joint exploitation of data, as well as the establishment of a specific infrastructure for the interconnection of data holders and data consumers; (2) between data subjects that want to make their personal data available and potential data consumers, thereby facilitating the data subjects to exercise their rights under the GDPR; and (3) services of data cooperatives particularly in the areas of micro, small, and mid-size enterprises.[52] The concept of notification does not imply an approval by the authorities,[53] but rather provides a mechanism to determine certain conditions for data intermediary services (before commencing their activity)[54] and to establish a supervisory control over an intermediary's compliance with such conditions,[55] which can impose "dissuasive financial penalties" (to be further defined by the Member States) if need be.[56] The EU Commission stressed that additional measures regarding rights on access and use of data are envisaged for the EU Data Act, as in discussion since February 2022.[57,58]

The conditions under Art. 11 Data Governance Act are of particular interest in the given context of IDS: the intermediary may not use the data it receives for other purposes than putting them at the disposal of data consumers; he/she shall not use the metadata collected from the data sharing service for other purposes other than developing that actual service, ensuring fair, transparent, and non-discriminatory access to the service for data holders and data consumers, including as regards prices; facilitating data exchange in the formats that the intermediary receives the data and converts data into other formats only to ensure interoperability within and

[50] Art. 5 paras. 2 and 4 Data Governance Act

[51] Art. 5 para. 11 Data Governance Act

[52] Art. 9 para. 1 lit. a–c Data Governance Act

[53] Art. 10 Data Governance Act

[54] Art. 11 Data Governance Act

[55] Art. 13 Data Governance Act

[56] *Spindler*: Schritte zur europaweiten Datenwirtschaft—der Vorschlag einer Verordnung zur europäischen Data Governance, CR 2021 p. 98–108 concludes that this results in a "general prohibition subject to a prior notification obligation." That appears rather drastic, whereas a notification obligation can indeed make sense, in order to create visibility for regulatory supervision (without, however, stipulating or accentuating the concept of a general prohibition).

[57] See https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-data-act. Accessed 10 February 2021.

[58] Proposal for a Regulation on harmonised rules on fair access to and use of data (Data Act), COM (2022) 68 final.

across sectors or if specifically requested by the data consumer, or if required under law, or to ensure harmonization with international or European data standards; preventing fraudulent or abusive practices; ensuring continuity of services and adequate technical, legal, and organization measures to prevent unlawful transfer or access to non-personal data; providing a high level of security for the storage and transmission of non-personal data; maintaining procedures to ensure compliance with competition law rules at the EU and Member State level; advising data subjects on potential data uses and standard terms and conditions attached to such uses; and advising on the relevant jurisdiction(s) of processing where an intermediary provides tools for obtaining consent from data subjects or permissions to process data made available by legal person.

From an IDS perspective, the Data Governance Act endorses the approach and key elements that IDS is promoting, including in particular the approach toward neutral intermediaries that rely on the reference architecture and the connector technology, in order to enable data sharing between data holders and data consumers in bilateral and multilateral data sharing ecosystems. The reference architecture and the information model of IDS are coherent with the requirements regarding data formats and interoperability. Operators of data spaces will need to pay particular attention, however, as to their monetization model. Under the current draft Data Governance Act, it appears excluded that an operator of a data space could generate innovative services through further-going metadata analytics, other than in order to "further develop" those data sharing services that the intermediary is actually providing to the specific data holders and data consumers concerned.[59] There are certainly good reasons to argue for such a limited remit, in respect to the definition of "metadata" that relates to the data holders and data consumers.[60] However, it appears important to discuss further clarity on whether an intermediary should not be able to generate ("anonymized") metadata aggregations and reports containing findings and learnings, as well as whether to use such data possibly as training data for machine learning, as long as the information contained in the actual metadata itself is properly protected and not shared with third parties for commercial gains or other unauthorized purposes.

Obviously, the Data Governance Act is subject to further debate, including the relatively generic requirements on security (currently not referencing state-of-the-art security but only referring to "high level of security,"[61] whereas, e.g., Art. 32 para. 1 GDPR shows a way to make sure a controller at least "takes into account the state of the art"). Further, it is important to bear in mind that the Data Governance Act represents only one part of legislation in regard to the European Data Strategy.[62]

[59] Art. 11 para. 2 Data Governance Act

[60] Art. 2 para. 4 Data Governance Act

[61] Art. 11 para. 8 Data Governance Act

[62] *Spindler*: Schritte zur europaweiten Datenwirtschaft—der Vorschlag einer Verordnung zur europäischen Data Governance, CR 2021 p. 98–108, noting, however, that Prof. Spindler does not touch upon the concept of data spaces as such in his wider considerations.

5.1.8 Personal and Non-personal Data

With its definition of personal data, the GDPR has determined an ample scope: "personal data means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, on online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."[63] Anonymization of personal data can enable a data controller to further process the data without considering the data protection requirements, provided that the data is no longer related to an identified or identifiable person.[64] Please note that pseudonymization of personal data (replacing identifiable personal data by a pseudonym) is reversible and can therefore only be used as an additional security safeguard for the processing. Examples such as IP addresses show that "personal data" is far more than might be obvious on first sight.[65] In addition, the rise of Big Data and AI has clearly shown that what might appear, at a given point in time, as anonymous data or other data with no connection or relevance to natural persons may actually turn out to be an element of personal data, once it is combined with other identifiers.[66]

However, the EU Commission has recognized the distinction by referring to "non-personal data" within areas of (limited) regulation, such as the Free Flow of Non-Personal Data Regulation.

Any concept regarding data spaces, such as IDS, must therefore be prepared to cater for compliance requirements regarding both personal and non-personal data.

---

[63] Art. 4 para. 1 EU Regulation (EU) 2016/679 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)

[64] See also Federal Commissioner for Data Protection and Freedom of Information: Position paper on anonymization under the GDPR with special consideration of the telecommunications sector. https://www.bfdi.bund.de/DE/Infothek/Transparenz/Konsultationsverfahren/01_Konsulation-Anonymisierung-TK/Positionspapier-Anonymisierung.pdf;jsessionid=47F123BF62DE633F32BB671CD74BAF74.2_cid329?__blob=publicationFile&v=2 (only available in German). Accessed 15 February 2021.

[65] Rec. (30) GDPR; p. 16 et seq. WP 29 WP136—01248/07/EN—Opinion 4/2007 on concept of personal data. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf. Accessed 28 January 2021; and ECJ C-582/14 Breyer v. Federal Republic of Germany

[66] "In most real-life situations, a dataset is very likely to be composed of both personal and non-personal data. This is often referred to as a "mixed dataset". Mixed datasets represent the majority of datasets used in the data economy and commonly gathered thanks to technological developments such as the Internet of Things (i.e. digitally connecting objects), artificial intelligence and technologies enabling big data analytics" (p. 8 EU Commission Guidance on the Regulation on a framework for the free flow of non-personal data in the EU https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019DC0250&from=EN. Accessed 28 January 2021; and p. 13 WP 29 WP136—01248/07/EN—Opinion 4/2007 on concept of personal data).

5.1.8.1 GDPR

From an IDS and data sharing perspective, the main question to be considered is which actors take which roles (controllers, processors, and joint controllers), in order to assess the related obligations. Additional considerations relate to the operators of data spaces in regard to the technical and organizational measures that they provide, in order to enable controllers and processors to share and process (personal) data in a data space.

The roles of data providers (acting as the [original] data controllers)[67] and data consumers (acting as [subsequent] data controllers) appear clear in a bilateral data sharing scenario, i.e., resulting typically in a controller-to-controller transfer and where the operator of the data space provides the infrastructure and takes the role of a data processor.[68] The data provider will need to assess the legal basis for making the data available to the data consumer under Art. 6 GDPR (e.g., consent of the data subject, performance of a contract with the data subject, legitimate interest) and ensure compliance with further obligations of a data controller (e.g., privacy notice under Art. 13 and 14 GDPR; safeguarding data subjects' rights under Art. 15 et. seq. GDPR, documentation obligations under Art. 30 GDPR, etc.). When it comes to scientific research—in particular in regard to special categories of data (e.g., health data, Art. 9 GDPR)—it may well be that data providers can claim specific legal justifications that the Member State legislators may have enacted, under the opening for national derogations.[69]

When it comes to multilateral data sharing, the data provider will need to consider the legal basis for providing the personal data concerned in regard to the data consumer separately—which may result in different legal basis applying, depending on the nature of processing, the various data consumers envision. Notably, the scope for "purpose variation" is limited under Art. 6 para. 4 GDPR.[70] Where the data provider relies on consent, he/she will need to provide appropriate consent management tools (including the option to withdraw consent); where he/she relies on legitimate interest, he/she will need to safeguard the right of objection.[71]

More complexity comes about where various data controllers jointly determine the purposes and means of processing personal data. This can occur in multilateral or consorted data sharing scenarios, either between the data provider and various data consumers or also (only) between various data consumers. In each of those

[67] Defined as the natural or legal person that "determines the purposes and means of the processing of personal data" (Art. 4 para. 7 GDPR)

[68] Art. 28 GDPR

[69] Art. 6 para. 2, Art. 9 para. 2 lit. g–j GDPR

[70] The [subsequent] data controller's processing purposes would need to maintain an inherent connection to the original processing purposes under which the [original] data controller had collected and transferred the personal data in the first place; in that context, notably, pseudonymization may provide a suitable safeguard (Art. 6 para. 4 lit. e GDPR).

[71] Art. 21 GDPR

scenarios, the parties involved will need to enter into a joint controllership agreement[72] and will assume joint and several liabilities for data protection compliance of their jointly controlled processing activities.[73]

The operator of a data space should put appropriate tools in the hands of data controllers, in order to ease the data providers' implementation of GDPR compliance. That can work by providing standardized documentation which the data controller(s) and processor(s) concerned can easily adapt and conclude as required—yet recognizing that a fully automated compilation of relevant documentation is very likely still a long way to go.

5.1.8.2 Free Flow of Non-Personal Data Regulation

The EU Regulation on the free flow of non-personal data[74] has two core objectives: ensuring the free movement of non-personal data across Member State borders, i.e., removing data localization requirements between Member States (and preserving availability and access to data for regulatory control purposes)[75] and easing the portability of data (in particular with regard to professional users switching cloud providers).[76] The regulatory approach on data portability is "soft-handed" and intentionally not interventionist, but self-regulatory, requiring further development through a "code of conduct" at the EU level.[77] From an IDS perspective, the relevant claim of data portability essentially regards the relation between the data provider and the operator of a data space. The data provider must have the option to move his/her account to another data space. IDS' reference architecture, the information model, and the data connector technology that allows to process and connect interoperable data formats are suitable measures to meet these requirements, which should therefore be instrumental in preparing related "code of conduct" under Art. 6 of the Free Flow of Non-Personal Data Regulation, if and when required.

5.1.9 Cybersecurity

The rise of cybersecurity threats is inherent to the growth of digital ecosystems and data sharing within data spaces. Clearly, robust cyber resilience and related organizational measures are a pre-condition for data providers and data consumers to share personal and non-personal data. However, it is also a question of regulation. The NIS

[72] Art. 26 GDPR

[73] Art. 82 para. 4 GDPR

[74] (EU) 2018/1807 of 28 May 2019

[75] Rec. (13) and (18) and Art. 4 para. 1, Art. 5 Free Flow of Non-Personal Data Regulation

[76] Art. 6 Free Flow of Non-Personal Data Regulation

[77] Art. 6 para. 1 Free Flow of Non-Personal Data Regulation

Directive and the Cybersecurity Act are key pillars of a European cybersecurity framework and are complemented by the requirements on technical and organizational measures in regard to personal data[78] as well as security measures required by data intermediaries.[79]

5.1.9.1 NIS Directive

The NIS Directive and its implementation into national security laws set the framework for adequate security of providers of essential services as well as digital service providers.[80] Besides the providers of essential services, the NIS Directive requires EU Member States to impose security requirements also on providers of digital services, which are defined as online marketplaces, online search engines, and cloud computing services.[81] Cloud computing services are defined as "a digital service that enables access to a scalable and elastic pool of shareable computing resources." The EU Commission has issued an Implementing Regulation[82] on the basis of Art. 16 para. 8 NIS Directive that specifies the security obligations of the providers of digital services. Accordingly, providers of essential services and/or digital services that fall within the scope of the NIS Directive will be able to use IDS, if and where they can define, configure, and rely on the security settings for data exchange.

5.1.9.2 Cybersecurity Act

The EU Cybersecurity Act (CSA) complements the provisions of the NIS Directive with additional regulations on the tasks and powers of the EU Agency for Network and Information Security (ENISA) and with the baselines of a new cybersecurity certification scheme for Information and Communications Technology (ICT) products services and processes. This cybersecurity certification scheme under Art. 51 CSA is still under development by the ENISA. On May 27, 2021, the Federal Government adopted and published its revised German IT security Act 2.0 (ITSiG 2.0). With the new ITSiG 2.0, the German Federal Offices for Information Security's powers is largely expanded and provisions inter alia regarding the storage of log

[78] Art. 32 GDPR

[79] Art. 11 para. 7 and 8 Data Governance Act

[80] In the future, subject to the updated version of the NIS 2.0 Directive ("NIS2"), as per the Council's and EU Parliament's adopted version of 13 May 2022. Notably, Member State implementations vary under the Directive, including the related level of sanctions and enforcement. Germany has implemented an enhanced "IT Security Act 2.0" on 27 May 2021 (anticipating some of the changes discussed at the NIS2 level subsequently), raising the bar of sanctions up to EUR 2 million (Section 14 para. 5 ITSiG 2.0).

[81] Art. 4 no. 5 and Annex III NIS-Directive

[82] Commission Implementing Regulation (EU) 2018/151 of 30 January 2018

data, inventory data disclosure, and implementation of detection measures for network and IT security are implemented.[83] Where regulated entities need to follow these requirements, IDS can potentially offer the architecture and framework for related compliance, noting, however, that it remains within the responsibility of the regulated entity/ies to define and implement their security requirements for related data exchange.

5.2 Preparing Contractual Ecosystems

The IDS sets out the landscape of participants in the ecosystems, and deriving from that, which participants need to bound through contractual agreements with other participants, in order to support the data exchange between the data providers and data consumers (Fig. 5.1).

The entire concept of IDS and data sovereignty is based on the principles of contract law, in order to ensure that data providers can determine and enforce the rules and conditions under which they share with and enable data consumers to use their data, be it in bilateral ("1:1") or multilateral usage scenarios ("1:1" and "1:*n*"). In that context, the fundamental principles of freedom of contract, including the freedom to choose the governing law, must always be at the disposal of the contracting parties.

IDS provides the framework and technology to allow the parties to limit their transaction costs and to ensure effective enforcement through the concept of usage control. In a future world, this will include increased automation of contract execution (conclusion, performance, and enforcement), whereas the steps to reach that goal are plentiful and, as of now, still require to "set the scene" with the means of traditional contractual agreements.

The following considerations explain some of the fundamental concepts and approaches for data licensing agreements, i.e., those agreements that data providers and data consumers will conclude, and how that can work on the basis of platforms that enable such data exchange. While the following explanations stand against the background of German law (and hence need to bear in mind that underlying statutory law can impact the formation and interpretation of contracts), they are to a considerable degree generic in nature and can be applied to other jurisdictions (even if adaptations under local law remain indispensable).

[83] Draft ITSiG 2.0 (9 December 2020) https://intrapol.org/wp-content/uploads/2020/12/IT-SiG-2.0-RefE-Stand-9.12.2020.pdf (only available in German). Accessed 28 January 2021

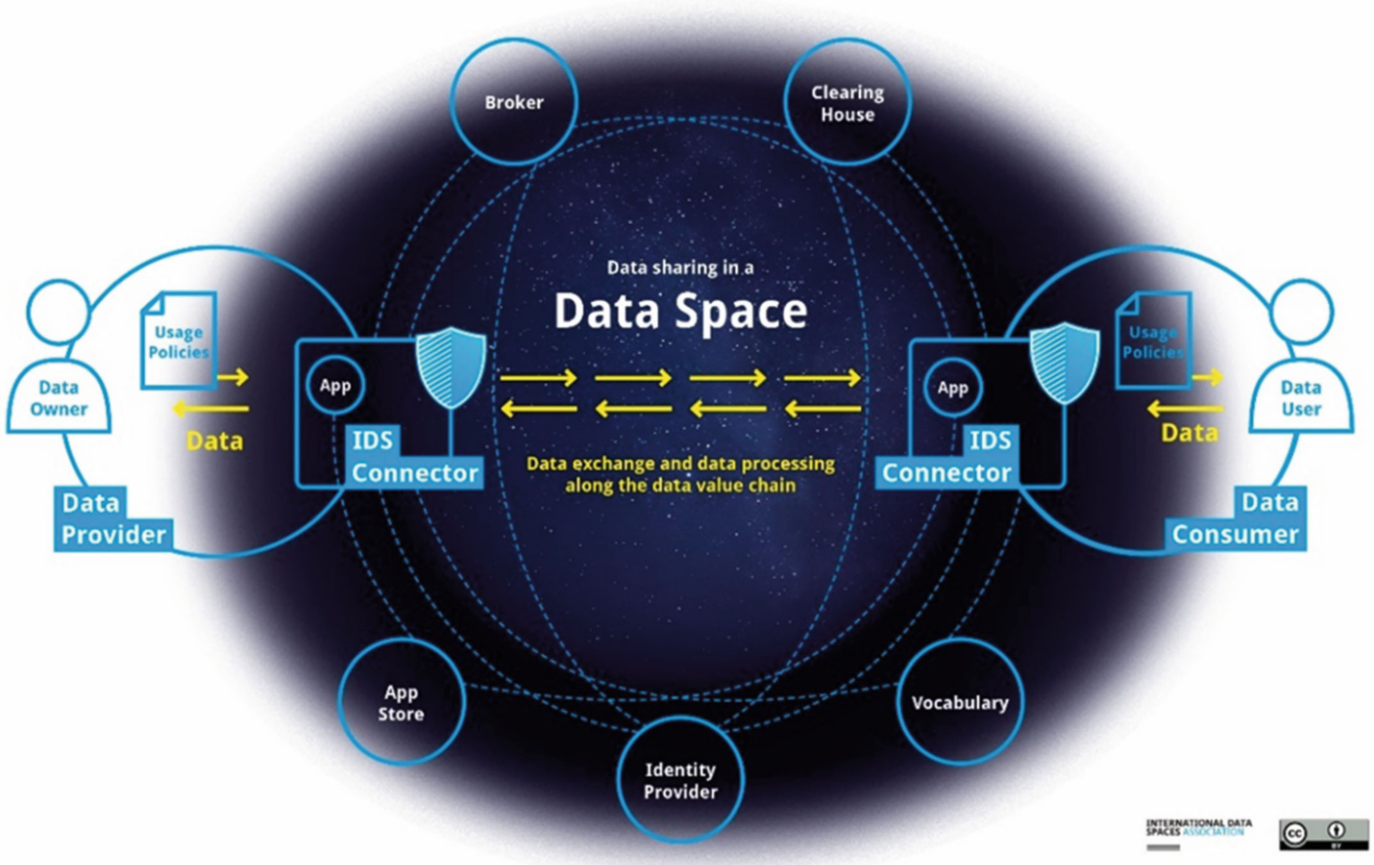

Fig. 5.1 Data sharing in a data space. © 2021, International Data Spaces Association [CC-BY]. Used under permission from International Data Spaces Association

5.2.1 Platform Contracts

As mentioned above, the role of intermediaries and, in particular, operators of platforms is key for the success of facilitating data exchange and accelerating the growth of the data economy.[84] Accordingly, it is important to consider the contractual setting that a provider of data connector services has to offer, possibly in first place and by which the data providers and data consumers can transact. That said, it is equally possible that data providers can do without the services of a platform provider, if and where they simply draw on the IDS connector technology and organize the data exchange (1:1 or 1:*n*) by themselves.

5.2.1.1 Key Principles

A platform operator that offers services to facilitate a data exchange will typically define its contractual relationship with data providers and data consumers by general terms and conditions, similar to those of other digital marketplaces. The platform operator will want to consider the following key constituent elements in this context: (1) the platform that provides the technical infrastructure and related services (including service levels) for a reliable and secure data exchange, but is not prescriptive as to the actual commercial and legal terms under which data providers and data consumers perform data exchanges; (2) the platform operator that may put at the disposal of data providers and data consumers template contracts to facilitate transactions and reduce transaction costs for the various types of data licensing transactions, including related compliance documentation (such as data processing agreements as required under the GDPR) and may provide technical mechanisms to facilitate automated or semi-automated contracting as well as facilities for contract negotiation; (3) the platform operator that will typically set out a registration process for data providers and consumers, as well as define an acceptance process for the platform operator's terms of use; (4) the platform operator that will set certain requirements for accepting policy frameworks (such as the IDS reference architecture, security settings, permitted usage and exclusions, requirements on IPR and GDPR compliance), codes of conduct, etc. that the data providers and data consumers have to follow; (5) remuneration and usage fees; (6) provisions on warranty and liability in regard to the functioning of the platform; (7) indemnities resulting from possible third-party claims raised against the platform operator resulting from the data providers' transactions conducted with data consumers; (8) provisions and limitations regarding the platform operator processing, using and retaining data exchanged through the platform by data providers and data consumers; (9) term and termination; (10) confidentiality; (11) GDPR compliance in the relation between the platform operator and the data provider/data consumer and between the data

[84] See also Sects. 5.1.4 and 5.1.7.

provider and data consumers; (12) IDS certification of the platform operator; and (13) choice of governing law and dispute resolution.

These many aspects to consider show that contractual frameworks of platform operators cannot be easily transformed into binary executables or simple "smart contracts," as well as that IDS-based platform operators need to resort to a predefined governing law and rules on dispute resolution (which can include online arbitration) in a particular jurisdictions. However, IDS can provide a template for platform operators. The sample "Terms and conditions of participation in an Industrie 4.0 platform" certainly gives a very good starting point and is available under a Creative Commons license.[85]

5.2.1.2 Legal TestBed: A Lead Example

As part of its activities, the legal working group of the "Plattform Industrie 4.0" has initiated a widely remarked "Legal TestBed" that is designed as a sand-box exercise for simulating a legal contract execution process (conclusion, performance, and enforcement) in an Industrie 4.0 context.[86] As part of the exercise, the working group has created the "Terms of use for an Industrie 4.0 platform" (Terms of Use), by way of an extensive drafting and consultation process among legal practitioners of academia, industry, and private practice. These Terms of Use are designed to ensure a reasonable balance between the interest of the platform operator and the users (data providers and data consumers), in order to facilitate data transactions and/or operational processes (such as performance of a logistics order and performance process) on the platform.

The Terms of Use cover the principles set out above (Sect. 5.2.2.1). By virtue and subject to the terms of the Creative Commons license, any third party is free to use and adapt these Terms of Use for its own platform operations.

5.2.2 Data Licensing Agreements

While building the data economy is a process that has only started, it appears that the commercial practice of data licensing is advanced in certain specific areas, whereas in other areas and sectors it is still largely "unknown territory." Accordingly, data licensing agreements do not yet follow general common standards that practitioners can "pull off the shelf," such as in the world of software licensing. In any event, therefore, it is helpful to be aware of the fundamentally different types of contractual

[85] https://www.plattform-i40.de/PI40/Redaktion/EN/Downloads/Publikation/RTB_contract_template.html. See the following chapter.

[86] For further information on the initiative, see https://legaltestbed.org/en/start/. Accessed 9 February 2021.

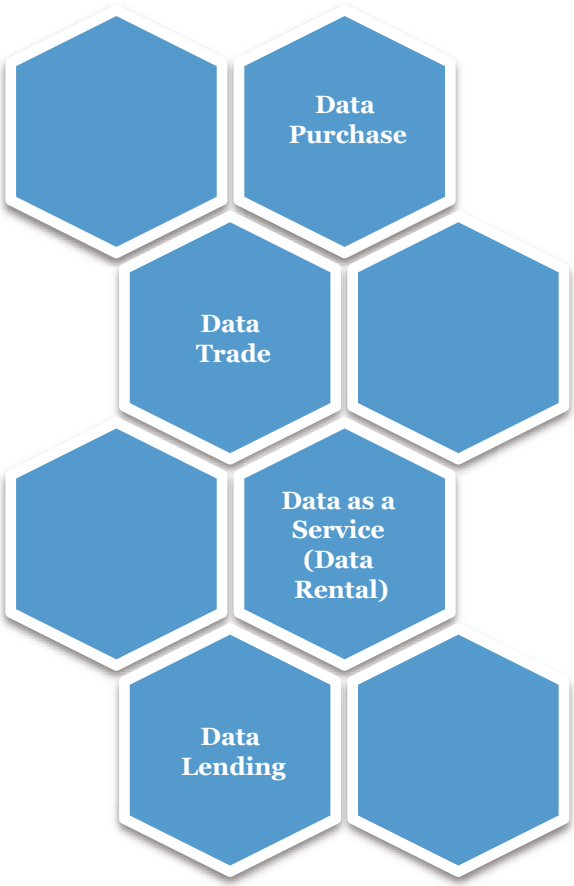

Fig. 5.2 Categorization of contract types. © 2021, Dr. Alexander Duisberg, Bird & Bird LLP

arrangements that data licensing transactions can follow. In simplified terms, the key distinctions that any data provider must consider are around the nature of the transaction, i.e., whether he/she intends to grant (1) perpetual or temporary, (2) exclusive or non-exclusive, and (3) royalty-free or paid-up usage rights—and in which combination of each of these aspects. From a German legal perspective (which can at least be helpful also for other civil law jurisdictions), the categorization of contract types can help in this regard (Fig. 5.2).

A "data purchase" implies perpetual (exclusive or non-exclusive) usage rights against a one-time remuneration. "Data as a Service" implies temporary (exclusive or non-exclusive) usage rights in data (comparable to a rental model), whereas "data lending" would imply that the lender asks for no compensation, and in a "data trade" the data provider would receive data as a non-monetary compensation. From a German law perspective, each of these different transactions falls in the category of a different contract type, to which the German Civil Code attaches different requirements, as well as contractual remedies in case of a breach. As a result, the

data provider needs to consider the legal consequences and risks involved when setting his/her contract terms against that background.

5.2.2.1 The Contract Matrix

The following matrix provides initial guidance (under German law) on the key elements to consider in relation to the various parameters applied to the different contract types. Some of these parameters are suited for a binary implementation (e.g., exclusive or non-exclusive usage rights, etc.) which therefore facilitates automated contracting (Fig. 5.3).

Obviously, any exclusive grant of usage rights is limited to 1:1 data licensing transactions—and would (potentially) even exclude further usage by the data provider, unless he/she explicitly reserves such rights. An important element to consider is the sui generis database right which is based on the (unique) EU Database Directive and its implementation to EU Member States laws.[87] A data provider that licenses structured data will need to consider the implications, i.e., whether and to which extent he/she defines limitations on the data consumer in creating new database rights by investing into substantively different methods of making datasets searchable.[88]

5.2.2.2 The IDS Sample Contracts

In addition to the "Terms and conditions of participation in an Industrie 4.0 platform," the IDS itself has developed two basic templates to cover data purchases and data as a service type of licensing transactions, designed against the background of German law and considering the particular implications of German rules governing standard terms and conditions. Again and as stated above, the intention of providing template agreements is not about being prescriptive, but rather to endorse the overarching principle of freedom of contract, whereas trying to reduce the transactional costs of setting up and negotiating suitable contracts for data licensing.[89]

[87] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases and Sections 87a et seq. German Copyright Act

[88] Art. 10 para. 3 EU Database Directive: "Any substantial change, evaluated qualitatively or quantitatively, to the contents of a database, including any substantial change resulting from the accumulation of successive additions, deletions or alterations, which would result in the database being considered to be a substantial new investment, evaluated qualitatively or quantitatively, shall qualify the database resulting from that investment for its own term of protection." Section 87a German Copyright Act: "A database whose content has been changed in a qualitatively or quantitatively substantial manner shall be deemed to be a new database insofar as the change requires a substantial qualitative or quantitative investment."

[89] See Sect. 5.1.

	Data Sale (Verkauf)	Data Trade (Tausch)	Data Donation (Schenkung)	Data as a Service (Data Rental) (Miete)	Data Lending (Leihe)
Contractual model	Perpetual transfer of data against one-off payment	Perpetual transfer of data without monetary consideration (e.g. data as consideration)	Perpetual transfer of data without consideration	Temporary transfer of data in return for a monthly fee; indefinite until notice of termination or specific contract term	Temporary transfer of data without any monetary or other form of consideration
Duration	Indefinite contract term	Indefinite contract term	Indefinite contract term	Specific contract term OR indefinite until notice of termination	Specific contract term OR indefinite until notice of termination
Usage rights	• Exclusive or non-exclusive • Geographically limited or unlimited • Restriction to agreed usage purposes	• Exclusive or non-exclusive • Geographically limited or unlimited • Restriction to agreed usage purposes	• Exclusive or non-exclusive • Geographically limited or unlimited • Restriction to agreed usage purposes	• Exclusive or non-exclusive • Geographically limited or unlimited • Restriction to agreed usage purposes	• Exclusive or non-exclusive • Geographically limited or unlimited • Restriction to agreed usage purposes
Licensing term	Perpetual/ unlimited in time	Perpetual/ unlimited in time	Perpetual/ unlimited in time	Temporary (specific contract term OR indefinite, but subject to notice of termination)	Temporary (specific contract term OR indefinite, but subject to notice of termination)
Sublicensing	• Sublicensable subject to contractual qualification, OR • Prohibition of sublicensing	• Sublicensable subject to contractual qualification, OR • Prohibition of sublicensing	• Sublicensable subject to contractual qualification, OR • Prohibition of sublicensing	• Sublicensable subject to contractual qualification, OR • Prohibition of sublicensing	• Sublicensable subject to contractual qualification, OR • Prohibition of sublicensing
Copying and distribution	• Copying, distribution and publishing of data or parts of data is prohibited, OR • Contractually permitted	• Copying, distribution and publishing of data or parts of data is prohibited, OR • Contractually permitted	• Copying, distribution and publishing of data or parts of data is prohibited, OR • Contractually permitted	• Copying, distribution and publishing of data or parts of data is prohibited, OR • Contractually permitted	• Copying, distribution and publishing of data or parts of data is prohibited, OR • Contractually permitted
Sui generis right of database maker	• Data Consumer's general prohibition to copy, distribute and publish <u>significant</u> parts of database • The same applies to repeated and systematic actions with regard to <u>insignifcant</u> parts of database • Parties are free to agree otherwise	• Data Consumer's general prohibition to copy, distribute and publish <u>significant</u> parts of database • The same applies to repeated and systematic actions with regard to <u>insignifcant</u> parts of database • Parties are free to agree otherwise	• Data Consumer's general prohibition to copy, distribute and publish <u>significant</u> parts of database • The same applies to repeated and systematic actions with regard to <u>insignifcant</u> parts of database • Parties are free to agree otherwise	• Data Consumer's general prohibition to copy, distribute and publish <u>significant</u> parts of database • The same applies to repeated and systematic actions with regard to <u>insignifcant</u> parts of database • Parties are free to agree otherwise	• Data Consumer's general prohibition to copy, distribute and publish <u>significant</u> parts of database • The same applies to repeated and systematic actions with regard to <u>insignifcant</u> parts of database • Parties are free to agree otherwise
Usage types	Known and unknown types of use depending on contractual restriction	Known and unknown types of use depending on contractual restriction	Known and unknown types of use depending on contractual restriction	Known and unknown types of use depending on contractual restriction	Known and unknown types of use depending on contractual restriction

Fig. 5.3 Contract matrix. © 2021, Dr. Alexander Duisberg, Bird & Bird LLP

That said, any parties wishing to use the connector technology and transact under the framework and reference architecture of IDS will need to include the reference to IDS and, in particular, recognize the requirements on certification.[90]

5.3 Implementing Compliance

Obviously, any participant in an IDS-based data exchange must be aware and ensure to take the appropriate measures to act in compliance with applicable laws, in particular with mandatory rules of data protection law (GDPR) and rules of competition law.

5.3.1 GDPR

The GDPR applies at any time where data providers share personal data, i.e., "any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person,"[91] triggering all the relevant provisions regarding a legal basis[92] and its limitations on purpose variation[93] and transparency through privacy notices,[94] ensuring data subjects rights,[95] documentation requirements,[96] and breach notifications.[97]

5.3.1.1 Controllers, Joint Controllers, and Processors

Data providers and data consumers will need to assess which type of relationship they will have, i.e., (1) whether the data consumer processes personal data as a new controller for its own purposes or (2) whether it is processing personal data together with the data controller for jointly defined purposes (i.e., acting as joint controllers). Where the data provider and the data consumer effect a data transfer to enable a new

[90] See Sect. 5.4 and Chap. 3 "Certification Process."
[91] See Sect. 5.1.8.
[92] Art. 6 GDPR
[93] Art. 6 para. 4 GDPR
[94] Art. 13, 14 GDPR
[95] Art. 15–21 GDPR
[96] Art. 30 GDPR
[97] Art. 33, 34 GDPR

processing purpose, the data provider must assess the legal basis for the transfer in accordance with Art. 6 or Art. 9 GDPR (the latter for special categories of personal data). While legitimate interest[98] is very often the suitable basis for transferring data for processing purposes that the data provider has predefined, this approach will not work where it is foreseeable that the data consumer wishes to process that personal data for arbitrary purposes which are unclear at the time of the transfer. Equally, it may be a significant challenge to rely on legitimate interest where a data provider shares personal data in a 1:*n* relation with a (possibly unknown) multitude of data consumers. Further, it is important to recognize that legitimate interest cannot serve as a legal basis when it comes to special categories of personal data (e.g., health data).[99] Accordingly, data providers and data consumers may also need to consider if and where they need to base data transfers and subsequent processing on the data subject's consent, and manage related consent management tools.

5.3.1.2 Documentation

Where the data provider and the data consumer(s) or various data consumers among each other pursue common purposes of data processing, they will need to enter into joint controller agreements under Art. 26 GDPR. Again, IDS can provide template documents that allow the parties involved to reduce their transaction costs in setting up and negotiating such agreements. Yet, the parties involved will need to at least define the substantive content (data categories concerned, recipients, processing purposes), whereas certain standard elements including the required technical and organizational measures[100] can (possibly) be incorporated by way of reference to the security standards provided by the platform operator.

The platform operator, by contrast, will normally act and position itself as the data processor who provides the technical facilities and, hence, effectively processes personal data on behalf of the various data controllers. Accordingly, the platform operator will provide (and the various data controllers can draw on) standard data processing agreements as required under Art. 28 GDPR, in which the parties involved (controllers and processors) will need to determine the data categories, data recipients, and processing purposes, as well as information on sub-processors and various other details, including the technical and organizational measures.

Further documentation requirements include that data controllers display the related privacy notices[101] and maintain proper records of processing activities.[102]

---

[98] Art. 6 para. 1 lit f GDPR

[99] Art. 9 GDPR does not provide such general legal basis, but only allows processing—without the data subject's consent—in limited circumstances, such as for research purposes in particular scenarios set forth under Art. 9 para. 2 lit. (j) GDPR in accordance with the national derogations set forth by the Member States.

[100] Art. 32 GDPR

[101] Art. 13, 14 GDPR

[102] Art. 30 GDPR

5.3.1.3 Breach Notifications

Where personal data breaches occur, the data controller(s) will need to assess the risk for the rights and freedoms of the data subjects and, if so, notify within 72 h the competent data protection authority and, in case of significant risks, also the data subjects.[103] In an environment of sharing personal data, this requires a clear allocation of responsibility and reporting back to the data controller. With the means of data processing agreements[104] and the usage control under IDS, each data controller should be well equipped to follow through with its notification obligations, i.e., preparing a report on which data has been affected by which incident, what consequences might arise from the breach, and which measures the controller has taken to mitigate the impact.

5.3.1.4 Enforcement and Sanctions

All stakeholders need to be aware of the significant level of fines that the GDPR attaches to non-compliance[105] and the increased enforcement actions taken by the data protection authorities.[106]

Obviously, the primary responsibility falls with the data controllers, but also data processors can be held liable, or even both, controllers and processors, can be held liable to pay damages to data subjects, jointly and severally.[107]

---

[103] Art. 33, 34 GDPR

[104] Art. 28 GDPR

[105] Up to 4% of the annual aggregate turnover of a data controller for certain breaches, such as failures regarding establishing the proper legal basis, ensuring data subjects' rights (Art. 83 para. 5 GDPR), and up to 2% for failures such as lacking proper documentation (Art. 83 para. 4 GDPR)

[106] The French data protection authority CNIL imposed a fine of EUR 50 million against Google Inc. for lack of transparency, inadequate information, and lack of valid consent regarding the ads personalization (https://edpb.europa.eu/news/national-news/2019/cnils-restricted-committee-imposes-financial-penalty-50-million-euros_en). The Italian data protection authority Garante imposed a fine of EUR 12,250,000 against Vodafone for unlawful processing of personal data of millions of users for aggressive telemarketing purposes (https://edpb.europa.eu/news/national-news/2020/aggressive-telemarketing-practices-vodafone-fined-over-12-million-euro_en). The Hamburg Commissioner for Data Protection and Freedom of Information imposed a EUR 35.3 million fine for data protection violations in H&M's Service Center (https://edpb.europa.eu/news/national-news/2020/hamburg-commissioner-fines-hm-353-million-euro-data-protection-violations_de). The Berlin Commissioner for Data Protection and Freedom of Information issued a fine of around EUR 14.5 million against Deutsche Wohnen SE for non-compliance with general data processing principles (https://edpb.europa.eu/news/national-news/2019/berlin-commissioner-data-protection-imposes-fine-real-estate-company_de). The State Commissioner for Data Protection in Lower Saxony has imposed a fine of EUR 10.4 million against notebooksbilliger.de AG. The company had been using video surveillance to monitor its employees for at least 2 years with no legal justification (https://edpb.europa.eu/news/national-news/2021/state-commissioner-data-protection-lower-saxony-imposes-eu-104-million-fine_de). Accessed 9 February 2021.

[107] Art. 82 paras. 4 and 5 GDPR

IDS itself does not take the role of a data controller or data processor. Accordingly each participant in the IDS ecosystem must be aware and take responsibility for its compliance with the GDPR—respectively assess in the first place if and to which extent it is willing and capable to process personal data in light of those requirements, or determine that its data contributions and data exchange shall exclude personal data from the outset.

5.3.2 Competition Law

One of the significant challenges that all participants to data sharing ecosystems need to be aware of and observe are the requirements of competition law, in regard to horizontal cooperations between competitors, "vertically" in downstream distribution models for data, as well as wherever the market position of a data provider (or data consumer) and the nature of the information could result in a distortion of markets and/or an abuse of a market dominant position.[108] Arguably, European competition law is only picking up with the challenges of the digital economy. The future EU Digital Market Act ("DMA") sets an important milestone in regulating platform operators that have the role of a "gatekeeper". The DMA will likely enter into force at the begin of 2023. While it is premature to assess the actual impact of this regulation, the sanctions (of up to 10% of a gatekeeper's aggregate annual revenues) give a strong message aiming at a fair data economy and preventing "data oligopolies". Platform operators exceeding a certain size (in terms of market valuation, numbers of users, etc.) will fall under the DMA.[109]

[108] See Art 101–109 Treat of the Functioning of the European Union TFEU; Art. 101 No. 1 TFEU: "...All agreements between undertakings, decisions by associations of undertakings and concerted practices which may affect trade between Member States and which have as their object or effect the prevention, restriction or distortion of competition within the internal market, and in particular those which: (a) directly or indirectly fix purchase or selling prices or any other trading conditions; (b) limit or control production, markets, technical development, or investment; (c) share markets or sources of supply; (d) apply dissimilar conditions to equivalent transactions with other trading parties, thereby placing them at a competitive disadvantage; (e) make the conclusion of contracts subject to acceptance by the other parties of supplementary obligations which, by their nature or according to commercial usage, have no connection with the subject of such contracts." Art. 102 TFEU: "Such abuse may, in particular, consist in: (a) directly or indirectly imposing unfair purchase or selling prices or other unfair trading conditions; (b) limiting production, markets or technical development to the prejudice of consumers; (c) applying dissimilar conditions to equivalent transactions with other trading parties, thereby placing them at a competitive disadvantage; (d) making the conclusion of contracts subject to acceptance by the other parties of supplementary obligations which, by their nature or according to commercial usage, have no connection with the subject of such contracts."

[109] A provider of core platform services shall be designated a gatekeeper if (a) it has a significant impact on the internal market (annual EEA turnover equal to or above EUR 7.5 billion in the last 3 financial years, or where the average market capitalization or the equivalent fair market value of the undertaking to which it belongs amounted to at least EUR 75 billion in the last financial year,

Beyond those generic principles it is clear that each participant in a data space must apply particular care in regard to the nature of information that it discloses and shares by way of a data exchange.[110] Accordingly, data providers and data consumers must take the necessary precautions to avoid that sensitive industrial information is disclosed which could allow entry into price ties, creating oligopolies, or induce coordinated behavior in breach of the applicable EU and national competition laws.[111]

5.4 Certifications from a Legal Perspective

While certifications are by nature a technical issue, they represent an important pillar for building trust in IDS. In that context, a few legal aspects play a significant role.

5.4.1 Role of Procedural Rules

IDS has not only created a certification standard,[112] but is presenting the same in conjunction with procedural rules of certification.[113] These procedural rules of certification are built on the procedural rules of the "Trusted Cloud" initiative of the Federal German government, which have been developed and published in a joint initiative of various stakeholders.[114] As such, they represent a well-developed,

---

and it provides a core platform service in at least three Member States); (b) it operates a core platform service which serves as an important gateway for business users to reach end users (more than 45 million monthly active end users established or located in the Union and more than 10 000 yearly active business users established in the Union in the last financial year); and (c) it enjoys an entrenched and durable position in its operations or it is foreseeable that it will enjoy such a position in the near future (Art. 3 Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act Proposal)).

[110] Consequently, unfair competition or anti-trust issues should also be assessed, such as the market relevance of the platform and whether certain mechanisms could, e.g., create a market barrier due to entry thresholds where certain organizations do not qualify or may be excluded.

[111] See Plattform Industrie 4.0 Result Paper Industrie 4.0—Implications for competition law: https://www.plattform-i40.de/PI40/Redaktion/EN/Downloads/Publikation/competition-law.pdf?__blob=publicationFile&v=8. Accessed 10 February 2021. As an addition regarding the EU Commission's guidance on private sector data sharing and the undertaking's access claim under competition law to a platform, see *Frenz*: EU-Digitalisierungsrecht. Datennutzung—Wettbewerb—Klimaschutz, EuR 2020, 210.

[112] See Chap. 3 "Certification Process" and https://internationaldataspaces.org/use/certification/. Accessed 10 February 2021.

[113] See https://internationaldataspaces.org/download/19008/. Accessed 15 February 2021.

[114] With courtesy and permission of the authors, see Rules of Procedure for Certification According to the Trusted Cloud Data Protection Profile for Cloud Services (TCDP) https://tcdp.de/data/pdf/15_Rules_of_Procedure_v1.0_EN.pdf. Accessed 10 February 2021.

reasonably balanced set of rules following common market standards to conduct certifications.

5.4.2 Additional Aspects

The issuance and management of the IDS certification standard can raise competition law aspects, if and when it develops to have a market-relevant impact. Accordingly, the IDS intends to enable further (commercially oriented) certification bodies to certify against the IDS standard in going forward at such point, whereas for the time being, the International Data Spaces Association (IDSA), acting as a non-profit organization on a mere cost basis) will currently act as the sole certification body.

Any entity seeking a certification ("applicant") will enter into a related agreement with the certification body (i.e., IDSA or in the future other certification bodies) to conduct the certification assessment in accordance with the procedural rules. The actual examination may be assigned to a separate examination body ("audit body"), which will act either as a sub-contractor of the certification body or, preferably in order to maintain organizational independence, through a separate contract with the applicant. As regards contractual liability, the certification body and the audit body will seek to exclude liability to the extent possible under German law (and related rules on standard contract terms, i.e., limiting liability for ordinary negligence to the "typically foreseeable damage"). In addition, such bodies will want and need to maintain a suitable general liability insurance.