STUDY

Requested by the JURI committee

European Parliament

IPR and the use of open data and data sharing initiatives by public and private actors

Policy Department for Citizens' Rights and Constitutional Affairs
Directorate-General for Internal Policies
PE 732.266 - May 2022

EN

IPR and the use of open data and data sharing initiatives by public and private actors

Abstract

This study analyses recent developments in data related practice, law and policy as well as the current legal framework for data access, sharing, and use in the European Union. The study identifies particular issues of concern and highlights respective need for action. On this basis, the study evaluates the Commission's proposal for a Data Act.

The study is commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs at the request of the Committee on Legal Affairs.

This document was requested by the European Parliament's Committee on Legal Affairs.

AUTHORS
Prof. Dr. Matthias LEISTNER, LL.M. (Cambridge), Ludwig Maximilian University Munich
Ref. iur. Lucie ANTOINE, Ludwig Maximilian University Munich

ADMINISTRATOR RESPONSIBLE
Mariusz MACIEJEWSKI

EDITORIAL ASSISTANT
Christina KATSARA

LINGUISTIC VERSIONS
Original: EN

ABOUT THE EDITOR
Policy departments provide in-house and external expertise to support EP committees and other parliamentary bodies in shaping legislation and exercising democratic scrutiny over EU internal policies.

To contact the Policy Department or to subscribe for updates, please write to:
Policy Department for Citizens' Rights and Constitutional Affairs
European Parliament
B-1047 Brussels
Email: poldep-citizens@europarl.europa.eu

Manuscript completed in May 2022

This document is available on the internet at:
http://www.europarl.europa.eu/supporting-analyses

DISCLAIMER AND COPYRIGHT

CONTENTS

CONTENTS 5

LIST OF ABBREVIATIONS 8

EXECUTIVE SUMMARY 10

1. INTRODUCTION AND BACKGROUND 21

2. DEVELOPMENTS IN OPEN DATA & DATA SHARING AND LEGAL CHALLENGES 23

2.1. Most recent and possible future developments 24

2.1.1. Data access and data quality as relevant bottleneck 25

2.1.2. Open data and data sharing: definitions and typology 26

2.1.3. Status quo: contract-based data sharing 28

2.1.4. The development of the European policy discussion 29

2.1.5. The legal discussion 29

2.2. Benefits and challenges of open data and for data sharing initiatives 31

2.2.1. Potential benefits of facilitating open data and data sharing 31

2.2.2. Evidenced market failures as indispensable prerequisite for regulatory action 31

2.2.3. Challenges for promoting open data and data sharing 32

2.2.4. The way forward 33

3. THE EXISTING ACQUIS COMMUNAUTAIRE AND NEED FOR ACTION 34

3.1. Access and portability rights 36

3.1.1. General Data Protection Regulation: access to and portability of personal data 36

3.1.2. Regulation on the free flow of non-personal data: self-regulatory approach for B2B cloud service portability 37

3.1.3. Open Data Directive: re-use of public sector information 39

3.1.4. Sector specific-regulation 39

3.1.5. Competition law 40

3.1.6. Proposal for a Data Governance Act 41

3.1.7. Proposal for a Digital Markets Act 42

3.1.8. Contract law 43

3.1.9. Summary 45

3.2. Intellectual property rights and their impact on data access, portability and re-use 46

3.2.1. Computer Programs Directive: interoperability and interfaces 46

3.2.2. Database Directive: potential obstacle to data access, re-use and portability? 47

3.2.3. General Copyright Law: exceptions and limitations for text and data mining 57

3.2.4. Trade Secrets Directive 58

3.3. Need for action 59

3.3.1. Database Directive 59
3.3.2. Interface with trade secrets protection 64
3.3.3. Personal vs non-personal data 65
3.3.4. Portability 65
3.3.5. Measures for enhancing interoperability 66
3.4. Summary 67
4. PROPOSAL FOR A DATA ACT 69
4.1. Introduction and general remarks 71
4.1.1. Comprehensive harmonisation and coordinated enforcement 72
4.1.2. General overlap problems and coherence of legal instruments 73
4.1.3. Private law enforcement and need for specification 74
4.1.4. The role of contract law and need for respective model or standard contract terms 74
4.1.5. Relation to the GDPR and the notion of personal data 75
4.1.6. Overlap with IP rights and protection of trade secrets 76
4.2. Business to Consumer and Business to Business data sharing (Chapter II & III) 77
4.2.1. General scope and objective 77
4.2.2. Data access 'by design/default' and information duties (Article 3) 85
4.2.3. Right of users to access and use data (Article 4) 85
4.2.4. Right to share data with third parties (Articles 5 and 6) 96
4.2.5. Obligations for data holders obliged to make data available (Chapter III) 101
4.3. Unfair terms related to data access and use between enterprises (Chapter IV) 105
4.3.1. Scope 105
4.3.2. General clause (unfairness test), Article 13 (2) 107
4.3.3. 'Black list', Article 13 (3) 107
4.3.4. 'Grey list', Article 13 (4) 108
4.3.5. Summary 108
4.4. Making data available to public bodies based on exceptional need (Chapter V) 109
4.4.1. Scope 109
4.4.2. Conditions for making data available 109
4.4.3. Compensation 110
4.4.4. The role of personal data 111
4.4.5. Competent authorities and cooperation 111
4.4.6. Summary 111
4.5. Switching between cloud and edge services (Chapter VI) 112
4.5.1. Scope: B2C and B2B 112
4.5.2. Overlaps with the proposed Digital Markets Act 113

4.5.3. Obligations of the data processing provider 113
4.5.4. Summary 115
4.6. International contexts non-personal data safeguards (Chapter VII – Article 27) 115
4.7. Interoperability (Chapter VIII) 116
4.8. Implementation and enforcement (Chapter IX) 117
4.8.1. Competent authorities 117
4.8.2. Private remedies and enforcement 118
4.8.3. The role of model contract terms 119
4.9. Database sui generis right (Article 35) 119
4.9.1. Exclusion of machine-generated data from sui generis protection 119
4.9.2. The Database Directive: additional need for reform 121
4.10. Evaluation and review (Article 41), ex-post evaluation plan 121
REFERENCES **123**

LIST OF ABBREVIATIONS

AI	Artificial Intelligence
API	Application programming interfaces
B2B	Business to business
B2C	Business to consumers
B2G	Business to Government
CJEU	Court of Justice of the European Union
FRAND	Fair, reasonable and non-discriminatory
G2B	Government to Business
GAFAM	Google (Alphabet), Amazon, Facebook (Meta), Apple, Microsoft
GDPR	General Data Protection Regulation
IaaS	Infrastructure as a Service
IoT	Internet of things
IP	Intellectual property

OECD	Organisation for Economic Co-operation and Development
P2B	Platform to business
PaaS	Platform as a service
PIMS	Personal Information Management Systems
SaaS	Software as a Service
SMEs	Small and medium-sized enterprises
SWIPO	Working group on switching cloud providers and data porting
TFEU	Treaty on the Functioning of the European Union

EXECUTIVE SUMMARY

Current developments, legal framework and need for action

In the first three parts of this study, we have comprehensively analysed recent developments in data related practice, law and policy as well as the **current legal framework** for use of data and for data sharing initiatives in the European Union. On this basis, we have identified and systematised certain issues of concern and highlighted the **respective need for action.**

With regard to the **Database Directive**, we have therefore **proposed**

- to **specify the conditions** of protection for machine-generated data;
- to **reform the exceptions and limitations**;
- to substantially **shorten the term of protection**;
- to introduce a **pre-emption clause** in particular with regard to national unfair competition law;
- to introduce a **compulsory licence regime**;
- to develop (non-mandatory) **model contract terms** for the allocation of sui generis rights in the context of data related bilateral and/or network contracts.

With regard to **trade secrets protection**, we have **proposed**

- in the context of new access, sharing, and use rights to distinguish between (more sensitive) business information pertaining to specific market information or information about the very parameters of competition as such on the one hand and general technical or creative know-how on the other hand in order to strike a **more precise balance** between access and use interests on the demand side and the interest of protection on the rightholders' side taking into account the public interest in free and undistorted competition;
- to develop **(non-mandatory) model contract terms** for the licensing of trade secrets and for allocating the 'ownership' in cooperative data sharing networks.

The Commission's proposal for a Data Act

In the fourth part of this study, we have evaluated the Commission's proposal for a 'Regulation on harmonised rules on fair access to and use of data (Data Act)' based on the need for action which we have identified in the first three parts of the study.

Introduction and general remarks

The Data Act constitutes an ambitious project and a courageous policy decision with the objectives to open certain markets related to the IoT and cloud sector, to define explicit provisions for data sharing on contractual basis as well as to reduce technical barriers and allow B2G data access in exceptional situations. In order to establish 'harmonised rules on fair access to and use of data' it is a remarkable achievement that the Data Act proposes **institutional, decentral structures (which**

from our viewpoint are typical for private law claims and should also be enforced accordingly) for data access, sharing, portability, and use, thereby going way beyond the current legal framework focused primarily on (more centralised) data and services governance.

The Data Act introduces five new instruments: first, the **user's right** – applying in B2C and B2B relations – to **access** and **use data** generated by IoT products and to **share** such data with third parties; second, an **unfairness test for B2B contract clauses** on data sharing which have been imposed on SMEs; third, a framework for **B2G data sharing** based on exceptional need; fourth, provisions on **switching between cloud service providers**, and, fifth, safeguards against **unlawful access to non-personal data held in the Union in international contexts**.

Some of these proposed instruments (data sharing, mandatory unfairness control of B2B contracts, cloud and edge service provider switching), in particular because of their **sweeping scope** (B2C as well as B2B), their **mandatory character**, and the **central role of the user** concerning the access and sharing rights, require fundamental scrutiny in light of the involved **impact on the principle of contractual freedom** as well as with regard to their impact on **free competition** and their **prospective efficiency**. Also, certain 'fine-tuning' is necessary with particular regard to the objective to **reduce market entry barriers for newcomers** (or at least not to erect new or heighten existing barriers to market entry), in the markets for IoT products and cloud services.

Overlaps, balances and consolidation

As a general remark on legislative technique, concerning the entirety of the currently planned instruments of the **'data package'**, the relation between the different existing and in particularly the newly proposed instruments, their purposes and their content **needs to be** further clarified and **consolidated**. If the involved intricate **overlap**, **consolidation** and **balancing** issues remain unsolved or unclear, they will be a major factor causing legal uncertainty (chilling effects) as well as possibilities for opportunistic behaviour in the upcoming years.

In our study we have made several proposals concerning such overlap, consolidation and balancing issues which we have addressed mainly by proposing certain changes to the substantive provisions of the Data Act and by proposing certain avenues for adequate contextual delineation. Also, we have made proposals in regard to necessary institutional consolidation in the area of public enforcement and its relation to **necessary private rights and enforcement mechanisms**, as otherwise there will be a manifest danger of overlapping and contradicting enforcement decisions of different competent authorities in different sectors, concerning both the level of the Member States and the level of the Union.

Relation to the GDPR

In particular, concerning the **processing of personal data**, the Data Act takes into account the entire 'toolbox' of the GDPR by referring to any legal basis foreseen in Article 6 GDPR (or Article 9 GDPR) instead of relying solely on the data subject's consent. Requiring consent in the sense of Article 6 (1) (a) GDPR – or under the even stricter standards of Article 9 (2) (a) GDPR – in each case would indeed considerably reduce the practical efficiency of the new data access and sharing rights due to the high standards, legal uncertainty and practical difficulties with the GDPR's concept of consent, in particular in regard to dynamically involving use scenarios as well as for uses based on relevant sensitive data. However, Article 6 (1) (f) GDPR as the obvious main alternative route to legal processing of IoT data in private settings, poses equally problematic issues concerning the **lacking**

legal certainty with regard to the balancing of interests. In this overall context it should always be borne in mind that the GDPR expressly pursues two – equally important – objectives consisting in the protection of natural persons with regard to the processing of personal data *and* the free movement of personal data.

In the context of the proposed Data Act, the broad definition of personal data in Article 4 (1) GDPR – which at the same time entails a *negative* definition of *non-personal* data – could be put under scrutiny. Large parts of the data processed in the data-driven economy relate (at some point) to an identifiable natural person or at least cannot always be clearly distinguished from non-personal data when larger or combined datasets are concerned. The same applies for data generated by IoT products: Location data (e.g. connected cars), use data (e.g. smart home devices) or search queries 'asked' to a virtual assistant can qualify in many cases as personal data in the sense of the GDPR. It might be necessary to **fundamentally specify the scope and impact of the GDPR in the sector**, i.e. to at least consider **amendments to the definition of personal data** in such scenarios in a way which is in line with the objective to improve the **free flow of sufficiently anonymised or manifestly publicly available data**, as well as to specify and clarify the specific possibilities to **balance** the legitimate objectives behind the Data Act with the fundamental right to protection of personal data by interpreting the respective heads for lawfulness of processing in Article 6 GDPR in accordance with the legal duties set out in the Data Act.

In this regard, our study, first, proposes certain ways to achieve the necessary and proportional balance, while preserving effective protection of personal data, and which can be implemented by **certain clarifications in the Data Act proposal** and without changing the text of the GDPR. Second, apart from these detailed proposals, one more fundamental aspect will be central to genuinely improve the conditions for businesses in the internal market in that regard in the future. As the Data Act aims at reducing the practical and technical barriers for data sharing by introducing standards for interoperability and other relevant technical features, in the context of the GDPR this could also be an occasion to further implement legally reliable **technical and organisational standards for the sufficient anonymisation of data**.

Relation to intellectual property rights and trade secrets protection

As regards the necessary balance with IP protection and trade secrets, the proposed provisions of the Data Act consequently and rightly focus primarily on potential overlaps with trade secret protection (particularly Chapter II, III) and with the sui generis right of database makers.

In principle, from the viewpoint of legal technique, the **relation to trade secrets** is satisfyingly addressed in Article 4 (3) and Article 5 (8). We have made further proposals to distinguish between (more sensitive) trade secrets relating to the very parameters of the competition process itself and (less sensitive) trade secrets in regard to technical know-how and other secret information not directly related to the very parameters of the competition process. From our viewpoint – for the sake of legal certainty – it should also be **clarified that the FRAND 'licences' (as they are foreseen in Article 8) will also have to define and cover necessary and justified use acts in regard to trade secrets**. This would be of mainly clarifying character as the necessary justification already follows from Article 4 (3) and Article 5 (8). However, it would also allow to take the character of certain data as trade secrets into account when further specifying the terms and range of FRAND compensation.

Database sui generis right (Article 35)

The difficult role of the database sui generis right in the context of data access, use and sharing has been comprehensively outlined in the third part of our study. We have demonstrated that the

database sui generis right has the potential to intensify de facto control over data, to aggravate existing access problems and to lead to hold-up issues in certain situations.

These issues are addressed (in a rather limited, cautiously delineated sector specific way) by Article 35. Pursuant to Article 35, the sui generis right 'does not apply to databases containing data obtained from or generated by the use of a product or a related service'.

While the explicit clarification that machine-generated databases do not fulfil the conditions of the sui generis right seems acceptable as a bright line rule to reduce the significant legal uncertainty concerning the conditions for protection in the sector, the wording and legal technique of Article 35 should be refined: Apart from certain necessary technical clarifications of the provision's wording it is recommended that it should be clarified (in the sense of a **Union law pre-emption doctrine**) that within the scope of the Database Directive, if a given database does not fulfil the conditions for protection, Member States shall be precluded to protect such a database on different grounds (such as *parasitisme* or unfair competition protection against misappropriation, unless additional factors, such as consumer confusion, warrant such additional unfair competition law based protection).

In fact, the restatement that machine-generated databases do not qualify for protection under the sui generis right solves some of the mentioned problems in regard to the conditions of protection by providing for a bright line non-conflict rule for certain cases. However, many of the problems we have identified in the first parts of this study and in earlier publications are not addressed by this very targeted provision. In this regard there is **still need for action**.

The role of private law enforcement

In general, the Data Act is characterised by broadly formulated standards ('general clauses') and many new legal concepts and terms. These provisions, terms and concepts will have to be further clarified and specified in the upcoming years. Since the Data Act – in particular in its central part on the introduction of new data access and sharing rights for users of IoT devices – assigns an important role to private agents' requests and bilateral or tri-lateral (contractual) agreements as a private law institution, the task to specify the proposed provisions should centrally lie with **private law courts**, thus should be addressed within **private law enforcement** and by private law courts instead of by a system of different intersecting public authorities. Therefore, in the interest of effective and proportionate enforcement it is **recommended to lay down express rules on private rights and litigation** and, more generally, on the substantive and procedural relationship between the public enforcement mechanisms, foreseen in Articles 31 et seq., and private litigation as the main pillar of putting this new regulatory framework into practice.

The proposed rules on B2C and B2B data access and sharing

From our viewpoint, the new system of proposed B2C and B2B data access, sharing and use in Chapter II and III is the central element of the Data Act. Besides the already mentioned necessity of **instruments for private enforcement**, our main concerns relate, first, to the **horizontal scope** and **generalising mandatory law character** of the proposed data access and sharing system, secondly to certain **inherent limitations** of that system, and thirdly to the **central role assigned to the users** in that new proposed system.

Scope and objective

The provisions proposed in Chapter II and III granting access and use rights for users and the right to share data with third parties in regard to data 'generated' by IoT products and related services are designed to constitute generally applicable, basic rules for all sectors in this field. Due to this **horizontal character covering the entire 'sector' of IoT products**, the proposed provisions, on the one hand, have a very broad scope of application – from industry to private use of connected products (**B2C and B2B alike**). On the other hand, in regard to the relevant data, the scope of the Data Act is limited to 'data generated by the use of products or related services' and thus does not substantially cover any **inferred or derived data**. Furthermore, the access to, use and sharing of these data is limited to uses **which do not compete** with the IoT product from which the data originate.

Consequently, these provisions can neither be consistently construed as addressing specific situations of abuse of dominant market positions (or other situations of specific market failure) nor as addressing specific situations of information asymmetry, imbalances in negotiation power (or other situations of specific contract failure). This is because under the perspective of situation-specific market failure or situation-specific contract failure, the scope and structure of these mandatory provisions would be at the same time both, too broad as well as too narrow. The scope of **mandatory law regulation is too broad** as these provisions obviously also apply in situations where no information or market power asymmetry can be identified at all. This is because, in particular **in B2B settings**, the user of the IoT product might as well be better informed and more experienced than the IoT product provider and data holder, and might also have a relatively stronger market position resulting in a relatively stronger negotiation position. In such a setting, broadly applicable, **sector-wide mandatory** provisions on data access and sharing cannot be justified as a corrective for a specific situation of market or contract failure. On the contrary, in some of these situations they might outright interfere with efficient, contract-based allocation of data, as because of their mandatory character, they prevent any reservation of data-related aftermarkets based on factual data control or contracts, even in situations, where this would be the efficient solution (e.g. a small newcomer (not a dominant undertaking) in the IoT producers' market could otherwise not enter the market at all) and would therefore benefit both parties to a respective contract. At the same time, the **scope is too narrow**, as we have identified situations of potential market failure in regard to the access to aggregated data, and, namely structured data, i.e. **contextualised, standardised data**, as the genuine main bottleneck for the development of many data oriented services at the moment. However, for such situations, the new provisions do not really provide a comprehensive remedy, because their **field of application is limited to volunteered and observed data** and their fundamental structure is oriented towards the access to and sharing of individual-level data (which at best indirectly and inefficiently helps to remedy situations where access to aggregate, contextualised datasets would be necessary and justified).

Instead of remedying specific situations of market or contract failure, the newly proposed provisions on data access, use and sharing in the Data Act are based on the general assumption that access to and use of IoT data in order to provide new products or services (in particular, but not only, maintenance, repair and other aftermarket services or products) will liberate aftermarkets and other new markets through the provision *and* commodification of data access rights, and will thus, in their total effect, create more benefits through enhanced dynamic efficiency than costs (through the undoubted interference with static and dynamic efficiency in certain situations, in particular B2B situations). The objective is thus to provide an **institutional framework for the development of certain new markets**, in particular in regard to new products or services in markets related to the

distribution of **IoT products** (such as repair, maintenance and other related markets), through generally opening and institutionally structuring hypothetical or actual upstream markets for the access to the necessary data generated by such products. This new regulatory approach, which goes way beyond the existing, comparably problem-specific approaches in competition law, consumer protection law and sector-specific regulation is at the same time limited in scope to IoT products and related (after)markets as well as in regard to upstream markets for volunteered or observed) data generated by the use of such products. Thus, while the regulated sector (use of any IoT product, B2C and B2B) is very broad and unspecific (**broad horizontal field of mandatory regulation**), the affected data categories (only volunteered and observed data, i.e. no inferred data) as well as the statutorily enabled uses (use for developing competing products is expressly excluded) are remarkably limited (**limited vertical depth of regulation**).

However, even in light of these crucial limitations, it has to be borne in mind that the sectors in which data-collecting IoT products are used, **vary widely**, and thus, the conditions on the relevant markets, the relationship between the actors and the amount and categories of the co-generated data differ significantly. Also, the aspect of possible new **barriers to market entry** (or at least chilling effects) for original producers which have not yet implemented IoT components in their products at all (and the general aspect of not chilling potential competition), should not be lost out of sight. General competition law by and large only sanctions market dominant firms for exclusionary conduct by leveraging their dominance on a primary market to a secondary market (although of course recent reforms, such as the most recent reform of the German Competition Act, have already cautiously departed from this approach inter alia in the context of the data economy). By contrast, the Data Act might be interpreted as a decision for generally opening (hypothetical) markets in the IoT sector through a **general ex-ante (market design) approach**, since from the viewpoint of the Commission the existing, competition law-based case-by-case analysis has turned out not to be effective enough to generally foster the development of certain data-driven markets. Even following this assumption, it would however also have to be shown, whether a generalised **mandatory law** framework (extending to all B2B-situations) is indeed required to reach this objective throughout the entire sector, whether solely opening secondary markets (by excluding data access, use or sharing in order **to compete** with the data holder) is sufficient and in particular, how such secondary markets shall be defined and delineated from situations of (direct) competition with the data holder in borderline cases. In that latter regard, the Data Act remains rather cautious, thus at the same time significantly limiting the impact of this new regulatory instrument for crucial case groups.

From our viewpoint, all this has three main general consequences resulting in two main policy recommendations. First, given the diversity of their field of application, the new provisions have to be re-evaluated with particular attention to their **scope** and necessary **flexibility** in particular through the use of flexible open-ended standards in the legislative text. Related to this on an instrumental level is the important question which institutional players shall specify these standards in the future as this will be crucial for the necessary balance between flexibility through the use of open-ended standards and fostering sufficient legal certainty through the specification of these standards in case law (this particularly also concerns the question of **private** and/or public **enforcement** and their relationship to each other).

Secondly, it has to be kept in mind that none of these new provisions should be designed, construed or applied in a way which puts disproportional **new cost burdens on newcomers** in the very markets the Data Act intends to open and incentivise (this particularly at least concerns necessary lenience in regard to SMEs as well as – again – the issues of the necessity of mandatory law, efficient

enforcement and necessary legal certainty which might be endangered if overlapping, multi-institutional public law enforcement causes significant additional administrative and information costs, e.g. because of resulting legal uncertainty and additional bureaucracy). As a **policy recommendation**, these two aspects lead to a need to **reconsider the broad scope** of the proposed mandatory framework (possibly in favour of a more sector-specific approach) and/or to re-evaluate whether **mandatory rules** are indeed needed in those B2B-constellations, where no manifest imbalance exists between the parties to the contract

Thirdly, one has to remain aware that **potential additional access problems**, which have been identified in the first part of this study, go way beyond the specific field of certain data co-generated by IoT products and the opening of related aftermarkets for products or services which are not in direct competition with the data generating IoT product itself. This is especially true for access needs of competitors to complete datasets for competing in secondary markets (which might include inferred data), and access to large aggregated datasets (e.g., training data and other **inferred data**) of big data conglomerates for innovation purposes (second and third case group) which might even lead to products or services which are in direct competition with the data generating product or service. Due to the strict **exclusion of services**, data generated by the use of (online) services or platforms are not covered by the proposed Data Act. This sector is therefore hitherto only covered in the 'data package' by the proposed Digital Markets Act, albeit limited to data held by gatekeepers (i.e. the GAFAM companies plus presumably less than a handful of other gatekeeper platforms) and to specific market situations. Therefore, it will be necessary to design and construe the new provisions in the Data Act in a way which allows the Act to at least indirectly contribute to the solution of some of these (partly related) data access problems. Also, it has to be kept in mind that the mentioned **access problems**, in particular in regard to aggregated, contextualised or standardised data and **in regard to certain larger (not purely data-processing, but data-driven) services**, might need to be addressed, going beyond the limited data related rights vis-à-vis Big Tech companies in the proposed Digital Markets Act. By contrast, the Data Act proposal is primarily designed to enable data access and use by third parties in a particular sector and in regard to but one central use scenario (aftermarket services for IoT devices). This leads to the **policy recommendation** to reconsider the **limitation of the scope** of the Data Act's proposed access and sharing regulation to IoT-products and related services, to re-evaluate the exact extent of the principled **exclusion of inferred data** as well as to reconsider the principled requirement of **non-competing use**.

The proposed central role of the user

Generally, and in particular for B2B constellations, it also needs to be justified why the **user** should be in a **central role**. Whereas protecting **personal data** by means of strong subjective rights (as provided by the GDPR) is mandated by the fundamental right to protection of personal data, the need for allocating mandatory access, use and sharing rights in regard to non-personal data to the users as suggested by the Data Act, is less self-evident. Allowing access to and use of data generated by IoT products and related services for **B2C relations** can also be seen as an expression of guaranteeing data sovereignty and 'empowering' of private consumers in regard to perceived information asymmetries or other reasons for an assumed weaker bargaining position of private consumers.

However, **in B2B constellations**, such allocation of non-personal data to the customers/users of IoT devices needs genuine justification. As we have explained, in B2B constellations, where the

customer/user is not a consumer, such mandatory allocation of data access, use and sharing rights, cannot across the board be justified by the identification of specific situations of market or contract failure – this would at best be possible for SME users vis-à-vis large IoT companies or for certain very specific sectors where empirical data clearly suggest the general actual or potential existence of such imbalanced situations. The Data Act goes beyond this, covering all B2B relations, where IoT products are used by businesses on the basis of sales, rental or lease contracts, alike. Thus, it seems that the mandatory allocation of data access, use and sharing rights to business users of IoT products is based on the perceived co-initiative and co-investment of such business users in the generation of the resulting use generated data through their actual use. As for the allocation of exclusive rights in such data, it has been decided by the CJEU in the context of the database sui generis right, that the mere generation of data in the course of another main business activity (i.e. as a spin-off of such a main business activity), shall not give rise to exclusive rights based on such more or less incidental generation of data. As for B2B situations under the Data Act proposal, the crucial (and somewhat different) question is whether the contribution to the generation of data through use of IoT products in the context of another main business activity, should give rise to certain limited and non-exclusive access, use and sharing rights for the user.

Whereas certain contextual elements in the *acquis communautaire* (in particular the conception of minimum use rights of the lawful user in the Computer Programs and the Database Directive) can serve as a tentative model for the access, use and sharing rights for business users in the Data Act, the crucial question remains whether the **initial allocation of such rights to the users** of the devices is efficient, when assessed in light of one of the main objectives of the Data Act, i.e. to create new markets for such data as a necessary precondition for the offer of new products and services in aftermarkets related to the originally distributed IoT product or its use. To answer this question, it will have to be considered, whether the users of such devices are sufficiently informed and incentivised to actually make use of their new rights, in particular also to share (and effectively market) them. In a rather limited field, i.e. the provision of specific new or at least cheaper or better services in aftermarkets, one might assume that the users as prospective customers of such services, might indeed be the best informed agents and might have sufficient incentives in order to initiate the necessary sharing of data by the data holder. At the same time effects, such as switching costs and inertia bias as well as the associated transaction costs, might well reduce the incentives of the users to effectively initiate data sharing. To make this envisaged regulatory system work, first, the relevant provisions of the Data Act must allow for **broad, non-static and transferrable as well as monetisable sharing claims** at least where trade secrets are not affected. Secondly – and more importantly – it will have to be considered whether the central (and to a certain extent 'proto-exclusive') role of the users in regard to initiating and authorising upstream data sharing is indeed as such justifiable and sufficient to effectively foster the emergence of dynamic and diverse new data markets as a precondition of new data related products or services.

In this context, it should also be kept in mind that the very generating, obtaining and observing of data generated by the use of a product or related service at the same time requires substantial ex-ante and continuous organisational, technical and financial efforts by the **data holders**. Also, in many situations, the data holders might be in a better situation to assess, negotiate and implement efficient data contracts, whereas the users' respective initiative and role seem less central and functional in that regard. In order to effectively incentivise data sharing, the role and legal as well as practical position of the **data holders (IoT producers and related companies) should therefore be equally taken into consideration, when regulating the sharing of such data on a non-exclusive basis** with third parties. In accordance with our analysis, we have made several proposals

to achieve this goal in our study some of which we also list in our following main policy recommendations.

Ex-post evaluation plan

We have been asked to also point at solutions, e.g. a data collection plan, which would allow for an ongoing evaluation of how legal solutions recommended in the study are implemented and if they are efficient and effective. In that regard **Article 41 foresees an *ex-post evaluation* of the Data Act** by the Commission *two years* after the date of its application with a particular view to certain adaptations of the central instruments of the Data Act. Indeed, such clause as well as any other provision injecting necessary flexibility and adaptability into the legal instrument seem highly recommendable in light of the very dynamic development of the regulated market sector. Art. 41 in principle provides a coherent basis for the evaluation of the Data Act and possible future adaptation although one might consider, in the interest of increased flexibility, whether in addition the Commission should also be empowered to make certain necessary mere specifications of open standards in the Data Act by way of delegated acts. As for possible ex-post evaluation and data collection, we have noted certain essential aspects in our study which we have summarised at the end of our following list of main policy recommendations.

In sum, we propose with regard to the **Data Act in general**,

- to **clarify and strengthen the role of private law enforcement**;
- to make the proposed public enforcement structures **optional** to the Member States and to streamline them, at best by a **one-stop shop** approach including a European 'meta-authority' for data related topics;
- to thoroughly assess the **coherence of the Data Act with the entire 'data package'** and the existing legal framework;
- to include provisions on the applicability of the Data Act in **multipolar settings** (e.g. data sharing networks) and to re-evaluate whether the current regulatory approach is well equipped to cover such situations;
- to **develop accompanying non-mandatory model contract terms**.

With regard to the proposed rules on **B2C and B2B data access, sharing**, **and use** we propose

- to **reconsider their broad scope of application and/or to critically evaluate the necessity of the mandatory character of the proposed system in B2B constellations** where no imbalance of the parties is present;
- complement the central role of the user with a **regulation of the position of the data holders**;
- to assess whether access to data generated by the use of **services** is already comprehensively covered by the proposed Digital Markets Act and to consider the **extension of the scope of the new data access, sharing and use rights to certain larger**

(not purely data-processing, but data-driven) services which are not gatekeepers under the comparatively strict thresholds of the proposed Digital Markets Act;

- to re-evaluate the exact extent of the principled **exclusion of inferred data**;
- to reconsider or at least to specify the conditions of the prohibition to use the respective data for developing a **competing product**;
- to consider whether the obligations to make data available set forth in the Data Act **could qualify as 'legal obligation' in the sense of Article 6 (1) (c) GDPR**, and, in the future, to consider further delineating the notion of 'personal data', at best by developing **technical and organisational standards for anonymisation** and by introducing a **rebuttable presumption** of anonymisation when the respective standards are met;
- to clarify that **FRAND 'licences' will cover necessary and justified use acts in regard to trade secrets**.

With regard to the **unfairness test for B2B contract terms** on data sharing we propose

- to specify that the fairness test does not apply to constellations in which a **micro or small business** is the imposer of a contract clause;
- to add the condition that a **gross imbalance** in the parties' rights and obligations arising under the contract must be the result of the unfair term.

With regard to **B2G data sharing** based on exceptional need we propose

- to reconsider whether the provisions should be **extended to small and micro-sized enterprises**.

With regard to the provisions on **switching between cloud and edge services** we propose

- to foresee an **exception for SMEs as providers**, at least for B2B relations;
- to revise the **relation to the proposed Digital Markets Act**;
- to **clarify the concept of 'functional equivalence'**.

With regard to the provisions on **interoperability** we propose

- to **extend the scope of the general principles** applicable to the operators of European data spaces to also guide future general standardisation processes in regard to cloud portability, data access and data sharing.

With regard to **Art. 35 on the database sui generis right** we propose

- to primarily 'refine' the wording of the provision in order to clarify that databases which fall into the scope of the Database Directive but which do not fulfil the substantive conditions of protection shall generally not be protected by other instruments of Member States'

national law either, absent any additional objectives entirely unrelated to the investment protection objective of the Database Directive (**Union law pre-emption doctrine**).

With regard to an **ongoing and ex-post evaluation** of how legal instruments proposed in the Data Act are implemented and if they are efficient and effective, we propose

- to carefully **choose certain very specific, carefully limited and representative industry sectors** for possible evaluation of central instruments of the Data Act and possibly associated data collection as otherwise the very broad scope and generalising character of the Data Act will prevent the emergence of conclusive results.

1. INTRODUCTION AND BACKGROUND

In the context of the Commission's proposal for a Data Act, the European Parliament Committee on Legal Affairs (JURI) has requested a study on '**IPR and the use of open data and data sharing initiatives by public and private actors**'.*

The Commission's proposal for a Data Act[1], which was planned to comprise a revision of the Database Directive[2], has already been announced in the Commission's Data Strategy of February 2020 as a further legislative step 'to provide incentives for horizontal data sharing across sectors'.[3] In May 2021, the Commission published the Inception Impact Assessment on the Data Act[4] which was followed by a Public Consultation open from June to September 2021.[5] In December 2021 the Commission presented a Summary report on the public consultation analysing the contributions of the 449 stakeholders which participated.[6] On 23 February 2022 the Commission presented its final proposal for a Data Act which is now subject to the feedback period open until 13 Mai 2022.

The Data Act is designed to complement the Commission's proposal for a Regulation on European data governance (Data Governance Act)[7] of November 2020.[8] On 30 November 2021, the European Parliament and the EU Member States reached a political agreement on the Data Governance Act concluding the trilogue negotiations.[9] The legal text of the Data Governance Act is now subject to formal approval by the European Parliament and the Council. The Data Governance Act aims at improving the availability of data by setting out rules for (1) the access to public sector data which are subject to rights of others (e. g. data protected as trade secret, by intellectual property rights or as personal data), (2) allowing personal data to be used with the help of data sharing services and (3) facilitating data use on altruistic grounds. Due to the complementary character of the Data Act, this study focusses on those aspects and case groups which are not already formalised by the Data Governance Act, notably the legal framework for sharing and re-use of private-sector data.

According to the Data Strategy and the Inception Impact Assessment, the Data Act has the following objectives: Facilitating and enhancing (1) B2G and (2) B2B data sharing, access and use, (3) expanding data portability rights in regard to personal and non-personal data, (4) establishing more

* We thank *Heike Schweitzer, Josef Drexl, Wolfgang Kerber, Axel Metzger, Ansgar Ohly, Tatsuhiro Ueno* and *Herbert Zech* for their consistently helpful comments and valuable ideas in our various discussions of the subject.

1 Proposal of 23 February 2022 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.

2 Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases (hereinafter 'Database Directive').

3 European Commission, *A European strategy for data*, COM(2020) 66 final, 2020, p. 13. The Data Act and the review of the Database Directive have been furthermore foreseen in the Commission's Work Programme 2021, *A Union of vitality in a world of fragility*, COM(2020) 690 final, 2020, Annex 1, p. 2, n. 6 and the Commission's *Intellectual Property Action Plan*, COM(2020) 760 final, 2020, p. 14.

4 European Commission, *Inception Impact Assessment Data Act*, Ref. Ares(2021)3527151, 28 May 2021.

5 See https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13045-Data-Act-including-the-review-of-the-Directive-96-9-EC-on-the-legal-protection-of-databases-/public-consultation_en.

6 European Commission, *Summary report on the Public Consultation on Data Act and Amended Rules on the Legal Protection of Databases*, Ref. Ares(2021)7509117, 6 December 2021.

7 Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act), COM/2020/767 final.

8 European Commission, *Inception Impact Assessment Data Act*, Ref. Ares(2021)352715, 2021, p. 1.

9 European Commission, Press release of 30 November 2021, https://ec.europa.eu/commission/presscorner/detail/en/IP_21_6428.

competitive markets for cloud computing services, (5) evaluating the use of smart contracts and (6) reviewing the role and impact of the Database Directive in this context.

This study's objective is to give policy recommendations addressed to the most relevant actors – including the European Parliament. It aims at providing summary, conclusions and recommendations on the proposed Data Act and in particular the revision of the Database Directive. For this purpose, the study explains the most recent and possible future developments in open data and for data sharing initiatives and provides an analysis of benefits and challenges of such initiatives (2.). It analyses the current legal framework for use of open data and for data sharing initiatives in the European Union and identifies and systematises issues of concern and respective need for action (3.). On basis of our results, we finally evaluate the Commission's proposal for a Data Act and suggest possible modifications (4.), taking into account the accompanying Impact Assessment Report[10] and the support studies[11].

[10] Commission Staff Working Document, *Impact Assessment Report*, Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), SWD(2022) 34 final. Concerning the state of play of the common European data spaces, see additionally: Commission Staff Working Document, *on Common European Data Spaces*, SWD(2022) 45 final, 2022.

[11] Deloitte and others, *Study to support an Impact Assessment on enhancing the use of data in Europe*, 2022; Sciadas, G. and Stavropoulos, P., *Methodological support to impact assessment of using privately held data by official statistic*, 2021; Calatrava Moreno and others, *Study to Support an Impact Assessment for the Review of the Database Directive*, Final Report, 2022; DORDA Rechtsanwälte GmbH and others, *Study presenting assessments of codes of conduct on data porting and cloud switching*, 2020. The *Study on model contract terms and fairness control in data sharing and in cloud contracts and on data access rights* has so far not been available.

2.DEVELOPMENTS IN OPEN DATA & DATA SHARING AND LEGAL CHALLENGES

KEY FINDINGS

In order to unleash the full potential of data-driven innovation, access to data and the quality of the available data are the pivotal elements. Not only AI applications but also (online) services, production processes, logistics, smart products, and targeted advertising are built on data input. The access not only to raw data, but in particular also to already aggregated data or combined training data (standardised or contextualised data as typical inferred data) in sufficient quantity, variety, and with adequate quality is decisive for both maximising the potential for obtaining optimal results and minimising risks, such as biases and discrimination.

Today, primarily service providers – being private companies or even public bodies – or manufacturers of machines and smart devices create and generate data. One key question is thus, whether and to what extent third parties (users, competitors, non-competing businesses, public bodies) can and particularly should get the possibility to access and (re-)use the respective data for further purposes, such as data aggregation, data analysis, or the provision of new services and products. Static efficiency and also aspects of dynamic efficiency argue in favour of broad access to data as a public good. At the same time, if access to data is granted too extensively, this can lead to adverse effects since the availability of certain sensitive information related to the very parameters of the competition process may effectively even restrict or distort competition; further, access rights might disincentivise investments in the effective production of inferred data or discourage competitors from collecting data themselves where this requires additional technical or organisational effort.

In accordance with these developments, the regulatory discussion on data has – both from the legal and policy perspective – shifted from a primarily incentive-oriented approach (which focused on establishing possible data 'property' rights) to a more competition and innovation-oriented analysis with main focus on the development of functioning data markets as both economic and legal evidence on the need for any (new) exclusive rights is lacking. As a result, the academic debate has identified three case groups in which data access, portability and re-use rights might be justifiable: *First*, access to individual-level use data (collected by a producer or service provider) and portability of such data. *Second*, access of competitors to complete sets of aggregated data, where this is necessary in order to establish workable competition in aftermarkets or complementary markets (in the primary market however solely under further conditions). *Third*, access to large aggregated datasets (e.g. training data) of big data conglomerates for developing unrelated products or services in new innovation spaces as parts of a digital ecosystem, in particular based on AI applications.

While these case groups are helpful to systematise possible situations where access, sharing and use rights might be justifiable, they do not as such justify them. On the contrary, empirical evidence, economic analysis, and ultimately a policy decision on that basis will always be required before introducing new data access, sharing and use rights.

Currently most data transactions are based on contractual relationships. However, designing respective contractual agreements which are workable in practice and legally certain is so far hampered by legal uncertainty as well as by significant transaction and information costs. This is particularly harmful to SMEs. As enhanced access and use of data by means of open data or data sharing have the potential to generate both economic and social benefits, at first sight, it might therefore seem desirable to facilitate data access and re-use as far as possible. However, (proven) efficiencies which can be achieved by disseminating data broadly have to be balanced against various other interest and policy concerns as well as the associated costs because of the inevitable interference with the principle of contractual freedom. In addition, not only legal barriers, such as most importantly the current legal uncertainty, have to be overcome but also further obstacles such as providing sufficient incentives for data sharing, addressing de facto control over data and reducing technical and organisational barriers.

2.1. Most recent and possible future developments

Digital technology and data-driven innovation has not only transformed economy and society in the last decade but has also become one of the corner stones of the European policy debate leading to different regulatory initiatives.[12] An increase of the global data volume of 530 %, from 33 zettabytes in 2018 to 175 zettabytes in 2025, is expected while the value of the data economy in the European Union in 2025 could already amount to € 829 billion (compared to € 301 billion in 2018).[13] From a European policy perspective, building a European data economy and creating benefits for the individual citizen but also achieving public objectives such as those formulated in the European Green Deal are at stake.

Due to the development of technologies, such as the Internet of Things (IoT), big data analytics and Artificial Intelligence (AI)[14], data-driven markets and business models today form the core of the envisaged 'European data economy'. Taking advantage of these technologies, e.g. by applying methods like machine learning, deep learning or evolutionary algorithms, requires huge amounts of data. Therefore, the access to data in sufficient quantity and quality is key for a data-driven economy. Cloud computing (and recent innovations as quantum computing) create the relevant technical infrastructure for using and managing the increasing amount of data. Due to cloud

[12] See inter alia European Commission, *Shaping Europe's digital future*, COM(2020) 67 final, 2020; European Commission, *A European strategy for data*, COM/2020/66 final, 2020; European Commission, *White Paper on Artificial Intelligence – A European approach to excellence and trust*, COM(2020) 65 final, 2020.

[13] European Commission, *A European strategy for data,* Factsheet, 2020, pp. 2 et seq., available at: https://ec.europa.eu/commission/presscorner/detail/en/fs_20_283.

[14] Identified as key technologies also by the OECD, *OECD Digital Economy Outlook 2017*, pp. 24 et seq.

services, computing power has also become available more flexibly and for cheaper prices enabling even SMEs to carry out large scale data processing. Many software tools used in AI are licenced under open-source terms or are at least available as open source versions which leads in principle to a far reaching availability of such tools. Therefore, neither computing power nor software itself can be qualified as prevailing obstacles for contributing to a data-driven economy.[15] Rather, the access to data, the possibility to (re-)use data and the adequate quality of data (including necessary meta-data) can be identified as relevant bottleneck as we will line out in the following.

2.1.1. Data access and data quality as relevant bottleneck

In order to unleash the full potential of data-driven innovation, access to data and the quality of the available data are the pivotal elements.[16] Not only AI applications but also (online) services, production processes, logistics, smart products, and targeted advertising are built on data input.[17] The access to raw data and already aggregated data or combined training data in sufficient quantity, variety, and with adequate quality is decisive for both maximising the potential for obtaining optimal results and minimising risks, such as biases and discrimination. But how can data be acquired?

Data is particularly obtained in three ways: by intentional sharing of data by the user (natural person or firm) of a product or service (*volunteered data*), by observing and capturing data automatically generated when using services or devices (*observed data*), and by analysing volunteered and observed data further (*inferred data*).[18] This distinction shows parallels to the different stages of data processing, starting with the collection/generation/acquisition of data, followed by their analysis (by means of big data analytics etc.) and further combination/aggregation (e.g. training data) which finally allows to make use of the found results, e.g. as knowledge base or basis for (automated) decision making (AI/machine learning/deep learning). Data itself can further be distinguished based on the level of systematisation and the character (raw data, structured and unstructured data, aggregated data, meta-data). Datasets can relate to only one single user, contain various individual user datasets or reach the level of aggregated data. The frequency of data generation varies, leading to *static* ('historic') *data* on the one hand and *real-time data* on the other hand.[19]

As a result, primarily service providers – being private companies or even public bodies – or manufacturers of machines and smart devices create and generate data. One key question is thus, whether third parties (users, competitors, non-competing businesses, public bodies) can and particularly *should* get the possibility to access and (re-)use the respective data for further purposes, such as data aggregation, data analysis, or the provision of new services and products. If access to data is granted extensively, this could indeed lead to adverse effects since the availability of

---

15 Crémer, J., de Montjoye, Y. and Schweitzer, H., *Competition Policy for the digital era,* p. 29.

16 European Commission, *A European strategy for data*, COM(2020) 66 final, 2020, p. 6.

17 Crémer, J., de Montjoye, Y. and Schweitzer, H., *Competition Policy for the digital era*, p. 73.

18 The classification goes back to a definition of the World Economic Forum, which was initially developed for personal data, see study *Personal Data: The Emergence of a New Asset Class*, p. 7. For a generalisation of this classification see Crémer, J., de Montjoye, Y. and Schweitzer, H., *Competition Policy for the digital era*, pp. 24 et seq.

19 This distinction is particularly relevant for the categories of observed and inferred data and the follow-up question whether and to what extent access and portability rights cover real-time data (see further below).

competitively sensitive information may restrict competition, access rights might disincentivise investments in the creation of data or discourage competitors from collecting data themselves.[20]

2.1.2. Open data and data sharing: definitions and typology

The most far-reaching approach for disseminating data is the concept of *open data* which aims at making data widely accessible and re-usable to different re-users without or under little restrictions and particularly without remuneration.[21] Open data policies are already applied by private companies[22] and (more often) by public sector bodies[23]. In the B2B sector, following an open data strategy could for instances be incentivised by a strong interest of the data supplier in the re-use of the provided data.[24]

A more targeted approach is *data sharing*. The term data sharing (as used by the European Commission) refers to data supply and data (re-)use in all possible forms and models.[25] Data sharing – just as data itself – is, however, a heterogenous concept as it may be voluntarily or obligatory, for free or against remuneration, take place in relation to users, competitors or other third parties, and be carried out directly or indirectly (e.g. via third parties).[26]

One form of data sharing is *monetising or trading data* based on *bilateral contracts,* either directly or via intermediaries, such as data marketplaces or data brokers.[27] *Data marketplaces* particularly play an important role where the data supplier does not know potential data re-users or is not willing to search for data sharing partners itself.[28]

Alternatively, data is shared and exchanged on *industrial data platforms* resulting from data sharing partnerships or networks.[29] Industrial data platforms can be defined 'as virtual environments

---

20 Crémer, J., de Montjoye, Y. and Schweitzer, H., *Competition Policy for the digital era*, pp. 92 et seq.

21 Expert Group for the Observatory on the Online Platform Economy, *Work stream on Data*, p. 30; OECD, *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-Use across Societies*.

22 Companies that follow an open data policy can often be found in the energy sector as in certain Member States a legal obligation to make energy data available exists, see Everis Benelux, *Study on data sharing between companies in Europe*, p. 64 and examples at p. 68. Further examples see in Commission Staff Working Document, *On the free flow of data and emerging issues of the European data economy*, accompanying the document Communication Building a European data economy, SWD(2017) 2 final, pp. 13 et seq.

23 See e. g. Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information ('Open Data Directive'). See further Capgemini Consulting, *Creating Value through Open Data: Study on the Impact of Re-use of Public Data Resources*. See as example the European Data Portal, https://data.europa.eu/en.

24 Staff Working Document, *Guidance on sharing private sector data in the European data economy*, SWD/2018/125 final, 2018, p. 5.

25 Staff Working Document, *Guidance on sharing private sector data in the European data economy*, SWD/2018/125 final, 2018, p. 1, 5.

26 Expert Group for the Observatory on the Online Platform Economy, *Work stream on Data*, pp. 21 et seq.

27 See for the following scenarios and respective examples further Staff Working Document, *Guidance on sharing private sector data in the European data economy*, SWD/2018/125 final, 2018, p. 5; Everis Benelux, *Study on data sharing between companies in Europe*, pp. 60 et seq.; OECD, *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-Use across Societies*.

28 Staff Working Document, *Guidance on sharing private sector data in the European data economy*, SWD/2018/125 final, 2018, p. 5.

29 The initiative 'The International Data Spaces Association' for instance has the objective to develop a global standard for international data spaces, see https://internationaldataspaces.org/wp-content/uploads/dlm_uploads/IDSA-brochure-International-Data-Spaces-Enabling-Data-Economy.pdf.

facilitating the exchange and connection of data between different organisations through a shared reference architecture and common governance rules'.[30] The conditions for sharing data on industrial data platforms vary, e.g. access to the platform is granted in exchange for an additional monetary remuneration or merely in return for providing data, leading to a mutual benefit from the data shared, limited to a restricted group of users,[31] designed for a particular sector or even for cross-sectoral data sharing. For the time being, however, B2B data sharing appears to take place especially within the same industrial sector.[32]

Data intermediaries can furthermore assume the role as a more 'neutral' and non-profit oriented actor, for instance as research repositories,[33] *trusted third parties* or *data trustees*[34]. In regard to personal data, similar solutions are discussed in the context of the 'MyData movement' which aims at establishing personal data storage and consent managing tools such as *Personal Information Management Systems* (PIMS). Data intermediaries, hence, can play very diverse roles in the data economy, from carrying out own commercial purposes to serving public interests and altruistic grounds. But it still remains to be seen how (and actually if) data intermediaries will develop in the markets and which role they will play in a data-driven economy.

A particular case group of data sharing is *data altruism* or *data donation*. Data altruism means making data accessible for purposes of public interest, e.g. scientific research, and refers to natural persons donating personal data as well as to businesses making data available.[35] For data intermediaries in general ('data sharing services') and organisations that facilitate data altruism, the planned Data Governance Act sets forth specific provisions, in particular notification and registration requirements, transparency obligations and supervision by the competent authority (see further below 3.1.6).

Even though not being a genuine tool of data sharing, *data portability* has to be considered as a complementary instrument for enhancing availability of data and fostering competition. Data portability describes the user's (natural person or firm) right to move, copy or transfer individual-level data when switching from one service provider to another.[36] Data portability aims not only at strengthening the control over individual-level use data but is also expected to increase competition and the users' choice as well as to foster the development of new products or services since it has the potential to minimise lock-in effects and lower switching costs.[37]

---

[30] This definition is used by Commission Staff Working Document, *On the free flow of data and emerging issues of the European data economy*, accompanying the document Communication Building a European data economy, SWD(2017) 2 final, p. 18 with reference to the IDC and Open Evidence study, *European Data Market Study – Industrial Data Platforms – Key Enablers of Industrial Digitization*, p. 8.

[31] In this case the implications arising from competition law have to be considered.

[32] Everis Benelux, *Study on data sharing between companies in Europe*, p. 94; Commission Staff Working Document, *On the free flow of data and emerging issues of the European data economy*, accompanying the document Communication Building a European data economy, SWD(2017) 2 final, 2017, p. 18.

[33] For an in-depth analysis see OECD, *Business models for sustainable research data repositories*.

[34] OECD, *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-Use across Societies*.

[35] See Staff Working Document, *Guidance on sharing private sector data in the European data economy*, SWD/2018/125 final, 2018, p. 12 for an example of B2G data donation.

[36] Commission Staff Working Document, *On the free flow of data and emerging issues of the European data economy*, accompanying the document Communication Building a European data economy, SWD(2017) 2 final, 2017, pp. 46 et seq.

[37] OECD, *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-Use across Societies*; Commission Staff Working Document, *On the free flow of data and emerging issues of the European data economy*,

2.1.3. Status quo: contract-based data sharing

Currently, most data transactions are based on contractual relationships.[38] However, designing respective contractual agreements which are both workable in practice and legally certain is so far characterised by legal uncertainty as only very basic guidelines for such data transactions exist (see further below 3.1.8.b). Moreover, describing integral parts of the contract, such as the exact subject matter, value and price, conformity and quality, conditions for access and use or contractual remedies is challenging due to the particular character of data.[39] In addition, the relevant infrastructure for realising data sharing transactions, data access, and data portability in practice – particularly interoperability and accessible application programming interfaces (APIs) – is widely lacking, thus constituting another main obstacle for fostering a European data economy.[40]

Hence, data sharing creates significant transaction and information costs, e.g. for identifying sharing partners that can provide relevant data, verifying data quality and data sources, negotiating contract terms, preparing data for sharing (validate, clean, structure), establishing the technical infrastructure for data sharing (import, export, transfer, storage, creating a 'data space' etc.), investing in skills, awareness and the 'cultural change' of a firm's internal organisation.[41] Businesses incur high entry costs as so far only little experience exists which is generally not shared with other stakeholders and, therefore, leads to a duplication of efforts.[42] Furthermore, often information on the provenance of data, their quality, type, size, or content is lacking.[43]

At the same time, imbalances in market power can be observed[44] resulting particularly from extreme returns to scale and strong network externalities.[45] As a result, unequal negotiation and bargaining power might in certain constellations have strong impacts on, first, whether a data sharing contract is concluded at all and, second, under which conditions.[46] However, due to the multifold data sharing scenarios – different actors, data categories, business models, sectors, and markets – it has to be examined thoroughly whether and in which case groups market failures can be identified leading to the need of regulatory action (see immediately below).

---

accompanying the document Communication Building a European data economy, SWD(2017) 2 final, 2017, p. 47 et seq.

38 European Commission, *Inception Impact Assessment*, Ref. Ares(2021)352715, 2021, p. 1; Staff Working Document, *Guidance on sharing private sector data in the European data economy*, SWD/2018/125 final, 2018, p. 6.

39 See for instance Staff Working Document, *Guidance on sharing private sector data in the European data economy*, SWD/2018/125 final, 2018, pp. 6 et seq.

40 European Commission, *A European strategy for data*, COM(2020) 66 final, 2020, pp. 8 et seq.; see from a competition law perspective Crémer, J., de Montjoye, Y. and Schweitzer, H., *Competition Policy for the digital era*, p. 16: 'The theme of interoperability appears in numerous places in our report, as we believe it to be one of the instruments that can keep markets open.' Everis Benelux, *Study on data sharing between companies in Europe*, pp. 75 et seq.

41 High-Level Expert Group on Business-to-Government Data Sharing, *Towards a European strategy on business-to-government data sharing for the public interest*, p. 25; Martens, B. and others, *Business to business data sharing: an economic and legal analysis*, p. 6.

42 High-Level Expert Group on Business-to-Government Data Sharing, *Towards a European strategy on business-to-government data sharing for the public interest*, p. 26 in regard to B2G constellations – however, the same holds true for B2B.

43 European Law Institute, *Response to Public Consultation on the Data Act*, pp. 19 et seq.

44 European Commission, *A European strategy for data*, COM(2020) 66 final, 2020, p. 8.

45 Crémer, J., de Montjoye, Y. and Schweitzer, H., *Competition Policy for the digital era*, pp. 20 et seq.

46 See answers to a survey concerning obstacles for B2B data sharing in Everis Benelux, *Study on data sharing between companies in Europe,* pp. 79 et seq. From a competition law perspective potential collusion or certain anti-competitive effects have to be considered in this context, see further Crémer, J., de Montjoye, Y. and Schweitzer, H., *Competition Policy for the digital era*, pp. 96 et seq.

2.1.4. The development of the European policy discussion

Since 2014[47] the Commission pursues the objective of developing a European data economy. As stipulated in the *Digital Single Market Strategy* of 2015[48] and sketched further with the Communication *Building a European Data Economy* of 2017, the Commission has highlighted the objectives of improving access to machine-generated data, facilitate and incentivise data sharing, and minimising lock-in effects but mutually protect investments and avoid disclosure of confidential data.[49] Along these lines, in 2018 – in the Communication *Towards a common European data space* – the Commission provided a set of key principles for both B2B and B2G data sharing.[50] With the *Data Strategy* of 2020[51], the objective of creating a Single Market for data was substantiated further amounting to improving access, use, and portability of data at a cross-sectoral level by providing a respective data governance framework, fostering interoperability by improving the relevant infrastructure for hosting, processing, and using data and developing European data spaces in strategic sectors and such of public interest.[52] These more detailed regulatory aims have found their first manifestation in the proposals for a Data Governance Act and for a Digital Markets Act of December 2020 (see further below).[53]

2.1.5. The legal discussion

The legal discussion has shifted from an incentive oriented institutional perspective which focused on establishing possible *data 'property' rights*[54] to a competition and innovation-oriented analysis with main focus on the development of functioning data markets in the EU as both economic and legal evidence on the need for any (new) exclusive right is lacking.[55] The specific actual and potential problems which might constitute obstacles for the development of functioning data markets have become the centre of the debate: *access* to data, *portability* of data with *interoperability* as key factor,

---

47 European Commission, *Towards a thriving data-driven economy*, COM(2014)442, 2014.

48 European Commission, *A Digital Single Market Strategy for Europe,* COM(2015) 192 final, 2015, p. 14.

49 European Commission, *Building A European Data Economy*, COM(2017) 9 final, 2017, pp. 11 et seq. See also the accompanying Commission Staff Working Document, *On the free flow of data and emerging issues of the European data economy*, SWD(2017) 2 final, 2017.

50 European Commission, *Towards a common European data space*, COM(2018) 232 final, 2018, p. 10. See more detailed the accompanying Staff Working Document, *Guidance on sharing private sector data in the European data economy*, SWD/2018/125 final, 2018.

51 European Commission, *A European strategy for data*, COM/2020/66 final, 2020.

52 Common data spaces are planned for the following sectors: mobility, manufacturing, health, financial, energy, agriculture, public administration, skills (education and labour market), and European Green deal, see European Commission, *A European strategy for data*, COM/2020/66 final, 2020, pp. 22 et seq. Their development is accompanied by the 'Support Centre for data sharing' which is provided and managed by the European Commission, see https://eudatasharing.eu.

53 Proposal of 15 December 2020 for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), COM(2020) 842 final (hereinafter 'Digital Markets Act'). On 23 November the Parliament's Internal Market and Consumer Protection Committee adopted its position on the proposal, see press release at https://www.europarl.europa.eu/news/de/press-room/20211118IPR17636/digital-markets-act-ending-unfair-practices-of-big-online-platforms. On 25 March 2022 the Council and the Parliament reached a provisional political agreement on the Digital Markets Act, see press release at https://www.consilium.europa.eu/de/press/press-releases/2022/03/25/council-and-european-parliament-reach-agreement-on-the-digital-markets-act/.

54 The European Commission's, *Public consultation on Building the European Data Economy*, 2017, was interpreted in this direction.

55 See e. g. Kerber, W., 'A New (Intellectual) Property Right for Non-Personal Data? An Economic Analysis', *Gewerblicher Rechtsschutz und Urheberrecht Internationaler Teil*, 2016, pp. 989 et seq.

infrastructure and *incentives* for data sharing and open data initiatives.[56] Consequently, the legal discussion focuses particularly on contract law, competition law[57] and the question of sector-specific users' access rights.[58]

In this context, consensus has been reached that possible future access and use rights will necessarily have to be justified in every specific case.[59] This means that, firstly, specific market failures have to be identified, secondly, it has to be established that only new access and/or use rights can serve as efficient remedies in regard to these specific market failures and, thirdly, it has to be shown that the positive effects of such new data access rights prevail compared to their costs. As a result, the academic debate has identified four main case groups in which data access, re-use and portability rights might be justifiable: First, access to individual-level use data (collected by a producer or service provider) and portability of such data.[60] Second, access of competitors to complete sets of aggregated data, where this is necessary in order to establish workable competition in aftermarkets or complementary markets (in the primary market however solely under further conditions). Third, access to large aggregated datasets (e.g. training data) of big data conglomerates for developing unrelated products or services in new innovation spaces as parts of a digital ecosystem, in particular AI.[61] Fourth, access to data generated by public bodies.[62] These

---

[56] Kerber, W., 'A New (Intellectual) Property Right for Non-Personal Data? An Economic Analysis', *Gewerblicher Rechtsschutz und Urheberrecht Internationaler Teil*, 2016, pp. 989 et seq.; Kerber, W., 'Governance of Data: Exclusive Property vs. Access', *International Journal of Intellectual Property and Competition Law*, 2016, p. 759; Drexl, J. and others, 'Position Statement of the Max Planck Institute for Innovation and Competition of 26 April 2017 on the European Commission's 'Public consultation on Building the European Data Economy''; Leistner, M., 'Big Data and the EU Database Directive 96/9/EC: Current Law and Potential for Reform', pp. 27 et seq.; Leistner, M., 'The existing European IP rights system and the data economy', pp. 209 et seq.

[57] Schweitzer, H. and Peitz, M., 'Ein neuer europäischer Ordnungsrahmen für Datenmärkte?', *Neue Juristische Wochenschrift*, 2018, p. 275 ; Schweitzer, H., 'Datenzugang in der Datenökonomie: Eckpfeiler einer neuen Informationsordnung', *Gewerblicher Rechtsschutz und Urheberrecht*, 2019, p. 569; Crémer, J., de Montjoye, Y. and Schweitzer, H., *Competition Policy for the digital era*; Kerber, W., 'Digital Markets, Data and Privacy: Competition Law, Consumer Law and Data Protection', *Gewerblicher Rechtsschutz und Urheberrecht Internationaler Teil*, 2016, pp. 642–643; Furman, J., Coyle, D. and others, *Unlocking Digital Competition – Report of the Digital Competition Expert Panel*; Richter, H. and Slowinski, P., 'The Data Sharing Economy: On the Emergence of New Intermediaries', *International Journal of Intellectual Property and Competition Law*, 2019, p. 4; see also Marsden, P. and Podszun, R., *Restoring Balance to Digital Competition – Sensible Rules, Effective Enforcement*.

[58] Drexl, J., *Data Access and Control in the Era of Connected Devices*; Schweitzer, H., 'Datenzugang in der Datenökonomie: Eckpfeiler einer neuen Informationsordnung', *Gewerblicher Rechtsschutz und Urheberrecht*, 2019, pp. 576–580.

[59] See from a regulatory perspective also European Commission, *A European strategy for data*, COM(2020) 66 final, 2020, p. 13 Fn. 39. In general, Commission Staff Working Document, *Better Regulation Guidelines*, SWD (2017) 350, 2017, p. 18.

[60] This case group phenomenologically corresponds to the concept of *co-generated data*, see in this regard particularly *ALI-ELI Principles for a Data Economy – Data Transactions and Data Rights*, Principles 18 et seq.; further European Law Institute, *Response to Public Consultation on the Data Act*, pp. 11 et seq.; see also European Commission, *Inception Impact Assessment*, Ref. Ares(2021)352715, 2021, p. 2.

[61] See for these three case groups Schweitzer, H., 'Datenzugang in der Datenökonomie: Eckpfeiler einer neuen Informationsordnung', *Gewerblicher Rechtsschutz und Urheberrecht*, 2019, pp. 572 et seq.; Crémer, J., de Montjoye, Y. and Schweitzer, H., *Competition Policy for the digital era*, p. 75 et seq. Some proposals also put case groups *two* and *three* together by suggesting data access rights where interests of the controller are outweighed by legitimate public interests or similar overriding considerations as far as further requirements are met (proportionality, access under FRAND conditions, protection of third-party rights, no-harm principle, reciprocity), see *ALI-ELI Principles for a Data Economy – Data Transactions and Data Rights*, Principles 24 et seq. and further European Law Institute, *Response to Public Consultation on the Data Act*, pp. 13 et seq.

[62] Richter, H. and Slowinski, P., 'The Data Sharing Economy: On the Emergence of New Intermediaries', *International Journal of Intellectual Property and Competition Law*, 2019, pp. 4 et seq.; Schweitzer, H., 'Datenzugang in der Datenökonomie: Eckpfeiler einer neuen Informationsordnung', *Gewerblicher Rechtsschutz und Urheberrecht*, 2019, p. 572; Richter, H., 'Zugang des Staates zu Daten der Privatwirtschaft', *Zeitschrift für Rechtspolitik*, 2020, pp. 245 et seq.

case groups will serve as basis for evaluating and structuring the following analysis of the current legal framework and for evaluating the Commission's Data Act proposal.

2.2. Benefits and challenges of open data and for data sharing initiatives

2.2.1. Potential benefits of facilitating open data and data sharing

Enhanced access and use of data by means of open data or data sharing has the potential to generate both economic and social benefits.[63] These benefits might consist in more transparency, accountability and empowerment of users, the chance for new business opportunities (in particular for SMEs), cooperation and competition across sectors and countries, crowdsourcing, new insights, user-driven innovation, and increased efficiency across society through data linkage and integration.[64] The European Commission further names the potential for innovation and job creation and the contribution to efficiency and international competitiveness of industries across all sectors.[65] From an economic perspective, data has become core element for the competitiveness of businesses and their possibility to contribute to innovation.[66] Data-driven innovation can foster the development of new products, services, business models, and markets. Society and the individual citizen may benefit from data-driven innovation, for instance through improved public health, personalised medicine, protection of the environment, modelling mobility and infrastructure, monitoring of energy consumption, predicting natural disasters, urban planning or even its contribution to the objectives of the European Green Deal.[67] Thus, also the private sector, governmental and civil society organisations and, in particular, users (including citizens) have an increasing interest in accessing and using data.

2.2.2. Evidenced market failures as indispensable prerequisite for regulatory action

Due to the potential benefits of improved availability of data at first sight, it might seem desirable to facilitate data access and re-use as far as possible. However, (proven) efficiencies which can be achieved by disseminating data broadly have to be balanced with various other interest and policy concerns, such as the freedom of competition and freedom of contract, the need for incentives to invest, of fundamental rights, protection of personal data, of intellectual property rights and of trade secrets, digital security and the reduction of societal, transaction or information costs.[68] Enhancing data access and use has to foster competition and innovation but also to safeguard private autonomy. Individual fundamental rights have to be considered as well as public interests and particular commercial purposes. On all levels and in relation to all relevant actors of data

---

63 OECD, *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-Use across Societies*.

64 OECD, *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-Use across Societies*.

65 European Commission, *Inception Impact Assessment Data Act*, Ref. Ares(2021)3527151, 28 May 2021, p. 1.

66 Crémer, J., de Montjoye, Y. and Schweitzer, H., *Competition Policy for the digital era*, p. 76.

67 European Commission, *A European strategy for data*, COM(2020) 66 final, 19 February 2020, p. 1; Drexl, J. and others, 'Position Statement of the Max Planck Institute for Innovation and Competition of 26 April 2017 on the European Commission's 'Public consultation on Building the European Data Economy'', p. 2; comprehensively OECD, *Data-Driven Innovation: Big Data for Growth and Well-Being*, pp. 27 et seq.

68 Crémer, J., de Montjoye, Y. and Schweitzer, H., *Competition Policy for the digital era*, p. 76; from a more general perspective OECD, *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-Use across Societies*.

transactions (B2C, B2B, B2G, G2B), sufficient (contractual) fairness, transparency, and accountability have to be secured. Market failures, lock-in situations, and hold-up potential should be avoided or remedied, where necessary, in order to guarantee workable competition in data markets. Concerning the internal market, actual or potential inefficiencies might also follow from regulatory fragmentation as such.

Most importantly, the efficiency of every regulatory intervention has to be put under strict ex-ante scrutiny for each case group. Any legal intervention, not only in form of mandatory but also of mere default rules, has a cost side which has to be considered when assessing the need for regulatory action. Overprotection and overlaps would all the more lead to high transaction and information costs, legal uncertainty, and thus less incentives to share data. Furthermore, efficient regulation has to bear in mind whether, where, and to what extent technical solutions can provide effective remedies or could at least complement legal intervention (e.g. data access control mechanisms, safeguarding confidentiality and privacy by encryption etc.).[69]

2.2.3. Challenges for promoting open data and data sharing

An imminent problem for enhancing data access and re-use is *de facto control over data.* While the possibility to exclude others from access to data and use of it – being a result of de facto control, exclusive or at least 'defensive' rights – has, on the one hand, the potential to incentivise investments in generating data as data holders fear 'free riding',[70] on the other hand, it can create considerable lock-in effects and market entry barriers, particularly for SMEs.[71] Existing IP rights can contribute to aggravating the problem of de facto control over data. The same holds true, albeit to a lesser extent, for trade secret protection. In order to tackle the problem of de facto control, one of the biggest challenges is setting sufficient incentives for data sharing.[72] In general, data sharing might for instance be incentivised by business models relying on economies of scale or making advantage of network effects, by the possibility to monetise data or by certain technical, reputational and public interest considerations.[73]

Further obstacles to data sharing can be categorised in legal, technical, and organisational ones:[74] Significant *legal uncertainty* is claimed in regard to the liability regime,[75] licensing, intellectual property rights and 'ownership',[76] unfair competition and anti-trust law (data sharing with certain

---

69 Reimsbach-Kounatze, C., 'Enhancing access to and sharing of data: Striking the balance between openness and control over data', pp. 50 et seq.

70 OECD, *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-Use across Societies*; Reimsbach-Kounatze, C., 'Enhancing access to and sharing of data: Striking the balance between openness and control over data', pp. 43 et seq.; Martens, B., 'Data access, consumer interests and social welfare – An economic perspective on data', p. 71.

71 Crémer, J., de Montjoye, Y. and Schweitzer, H., *Competition Policy for the digital era*, pp. 87 et seq.

72 Reimsbach-Kounatze, C., 'Enhancing access to and sharing of data: Striking the balance between openness and control over data', pp. 42 et seq.

73 Expert Group for the Observatory on the Online Platform Economy, *Work stream on Data*, pp. 19 et seq.; Everis Benelux, *Study on data sharing between companies in Europe*, pp. 39 et seq.

74 See European Commission, *Inception Impact Assessment*, Ref. Ares(2021)352715, 2021, p. 8.

75 Of particular importance also for B2G data sharing, e. g. when a wrong or discriminatory decision of a public body is based on inaccurate or biased data obtained from the private sector, see High-Level Expert Group on Business-to-Government Data Sharing, *Towards a European strategy on business-to-government data sharing for the public interest*, p.26

76 Everis Benelux, *Study on data sharing between companies in Europe*, p. 75.

partners as anti-competitive behaviour),[77] data protection law and the control of downstream use[78] leading to chilling effects[79] but also to information and transaction costs with regard to the contract design.[80] Moreover, data holders fear the disclosure and unlawful use of information/data, data breaches and non-compliance with trade secrets of data protection law. The lacking infrastructure and interoperability for data sharing but also issues of cybersecurity constitute important *technical barriers,* as 'standardised' data, ready for transfer and use, are typically not available (often not even for effective data sharing between different subsidiaries of larger groups of companies). From an *organisational perspective*, unequal bargaining and negotiation power, business-internal difficulties, lack of control over downstream use, and non-availability of skilled labour are further obstacles which have to be overcome for incentivising data sharing.[81]

2.2.4. The way forward

Promoting data sharing and open data requires a closer look at the identified legal, technical and organisational barriers. From a *legal* perspective, reducing the current legal uncertainty is key. The existing acquis communautaire already provides a comprehensive legal framework for both protecting the interests of the data holder – particularly by means of the database sui generis right and trade secret protection – and safeguarding the interests on the demand side by granting data access and use rights in particular cases (e.g. sector-specific regulation), by sanctioning anti-competitive behaviour and by allowing for data transactions on contractual basis. Hence, the actual need for regulatory action has to be assessed carefully and precisely following a competition and innovation-oriented analysis which focuses on the development of functioning data markets. There is no 'one size fits all' solution as data itself, data markets, business models, the actors, and the potential for market failures vary widely.[82] While *organisational* barriers as such cannot directly be remedied by regulatory intervention, reducing legal uncertainty in regard to data transactions might at least alleviate them partially. Any initiative, however, has to be accompanied by means for encouraging the development of an effective *technical* infrastructure for facilitating data flows in practice, such as interoperability through accessible interfaces and API and standardisation, e.g. in form of open standards.[83]

---

77 Concerning G2B constellations Articles 11 and 12 Open Data Directive therefore generally prohibit exclusive arrangement and stipulate the obligation to share data under fair and non-discriminatory conditions.

78 Everis Benelux, *Study on data sharing between companies in Europe*, pp. 76 et seq.

79 OECD, *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-Use across Societies,* p. 74 et seq.

80 Everis Benelux, *Study on data sharing between companies in Europe*, pp. 77 et seq.

81 See European Commission, *Inception Impact Assessment*, Ref. Ares(2021)352715, 2021, p. 2, 8; European Law Institute, *Response to Public Consultation on the Data Act*, 2021, pp. 20 et seq.

82 Crémer, J., de Montjoye, Y. and Schweitzer, H., *Competition Policy for the digital era*, p. 74; OECD, *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-Use across Societies*.

83 In this context the Commission has recently announced major investments in technologies needed for creating European common data spaces as defined in the Data Strategy including the development and availability of APIs, standards and compatible data formats (see European Commission, *Implementing Decision on the financing of the Digital Europe Programme and the adoption of the multiannual work programme for 2021 – 2022*, Annex, C(2021) 7914 final). Looking at the infrastructure for data sharing an additional layer is added by the need for cybersecurity standards which the Commission has already addressed with the Cybersecurity Act enacted in 2019 (Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 ('Cybersecurity Act')).

3. THE EXISTING ACQUIS COMMUNAUTAIRE AND NEED FOR ACTION

KEY FINDINGS

The existing acquis communautaire already provides for a comprehensive legal framework for protecting the interests of the data holders – particularly by means of the database sui generis right and trade secret protection. At the same time, it safeguards the interests on the demand side by expressly granting data access and use rights in certain cases (e.g. GDPR, certain contractual instruments, sector-specific regulation), by sanctioning anti-competitive behaviour (Art. 102 TFEU) and by generally allowing for data transactions on contractual basis.

On the data holders' side, data collections can be protected (in certain cases) through the database maker's sui generis right or (more generally) as a trade secret. Whereas the Trade Secrets Directive provides a sufficiently flexible instrument (with only certain, mostly more practical contract and enforcement related shortcomings), the database sui generis right as foreseen in the Database Directive has the potential to aggravate access problems and to intensify de facto control over data. Due to its broad scope, it can in principle be invoked by the rightholder against access and portability rights – even though in practice the sui generis right might only have rather limited impact. In particular, there is significant legal uncertainty in regard to core elements of sui generis protection, such as the distinction between collection and creation of data, the notion of 'substantial part' and other.

Access to and portability of individual-level use data (first case group) is provided for personal data primarily through Article 20 GDPR and for non-personal data in the context of B2C contracts for the supply of digital content or digital services through Article 16 (4) Digital Content Directive. For business users so far no general data access or portability right exists, unless foreseen in certain sector specific regulation. Apart from that, access to co-generated data is currently not granted in relation to service providers other than gatekeepers (by the proposed Digital Markets Act). General competition law, namely Article 102 TFEU, may apply where refusing access to data amounts to an abuse of a dominant position. Horizontal data access of competitors to complete sets of aggregated data necessary for workable competition in aftermarkets, complementary markets or even in the market of the data holder (second case group) is hitherto primarily governed by general competition law.

In light of the existing legal framework and the recent developments in practice, law and policy we have identified need for action. First, the Database Directive and the database sui generis right are in need of reform. The conditions of protection – most importantly for machine-generated data (IoT, but also certain services) – have to be specified in order to reduce legal uncertainty.

In addition, the exceptions and limitations should be revised as the sui generis right's limitation to the use of substantial parts and the existing limitations do not suffice for facilitating the re-use of data in the identified case groups of justifiable access to data. Furthermore, the allocation (ownership) of the database sui generis right, the term of protection, and the interface with national unfair competition instruments in some Member States law should be put under revision. As one remedy we have inter alia proposed to introduce a compulsory licensing regime for certain cases.

As regards the relation of data access and use rights to trade secrets protection, a more nuanced approach is necessary. The protection of trade secrets is justified insofar as incomplete information is a substantial condition for functioning and competitive markets, where such trade secrets concern market information or other information on the very parameters of competition. Beyond that (e.g. technical know-how), trade secrets protection serves the purposes of reducing transaction cost (inefficient factual protection measures) and fostering contractual sharing of information. On this basis, it has therefore to be carefully assessed whether and under which conditions access to (secret) information should be granted and whether, under which conditions (e.g. FRAND licences) and to what extent an 'access regime' should also cover the subsequent use of the respective information. In that regard, we have suggested that information on the very parameters of competition is more sensitive than trade secrets relating to know-how and other information which do not directly relate to the competitive process as such.

The relation of access rights to the GDPR is an overall problematic issue. It should be considered to define the notion of personal data more specifically in sectors where access to industrial and technical data is predominantly concerned. This could also entail providing for standards concerning technical and organisational measures for the reliable anonymisation of data and complementing this with at least a rebuttable presumption of sufficient anonymisation when businesses comply with such established anonymisation standards.

Moreover, enhancing data sharing and data portability in practice, largely depends on the technically, organisationally and legally effective feasibility. Therefore, laying down non-mandatory contractual model clauses for certain case groups is recommended to reduce transaction costs (in particular information costs also in order to raise the level of trust in particular of SMEs). Also, and as a general key element for any effective data transfer in the future, effective measures for enhancing technical and organisational interoperability have to be introduced.

In the following section we will give an overview of the existing European legal framework. First, we will focus on existing access and portability rights in EU law (3.1). Secondly, we will analyse intellectual property and trade secrets law with particular regard to its relevance for sharing with and subsequent use of data by third parties and with respect to its 'infrastructural' role for interoperability (3.2). Thirdly, in light of our typology of necessary data access case groups and the existing legal framework, we will identify need for action (3.3).

3.1. Access and portability rights

3.1.1. General Data Protection Regulation: access to and portability of personal data

For *personal data*, which is defined as any information relating to an identified or identifiable natural person, Article 20 of the General Data Protection Regulation[84] provides for an explicit data portability right of the data subject. Article 20 GDPR has primarily the objective to strengthen the data subject's control over personal data (see Recital 68 GDPR). However, the provision furthermore aims at reducing lock-in effects by facilitating the data subject's change between different service providers (as 'pro-competitive side-effect'[85]). As a result, Article 20 GDPR has become a condensation kernel for the general discussion whether portability rights should be extended widely or at least for specific sectors/case groups.

Article 20 GDPR applies where personal data is processed on basis of the data subject's consent, Article 6 (1) (a) GDPR, or on basis of a contract, Article 6 (1) (b) GDPR. The portability right thereby covers only data which the data subject has 'provided', hence, solely volunteered and observed personal data.[86] On the contrary, inferred data and real-time data are not governed by the GDPR's portability right. However, these data categories might be of the data subject's particular interest, for instance because real-time data constitute an essential basis for certain services (multi-homing, offering of complementary services) and inferred data (e.g. preferences, reputation data on platforms, etc.) are of specific 'value' for the data subject when switching to another service provider.[87] Even though the GDPR's portability right follows from the data subject's fundamental right to protection of personal data (Article 8 Charter of Fundamental Rights), due to its pro-competitive purpose, Article 20 GDPR reflects to a certain extent the ratio underlying the first case group (data access to (personal) individual-level use data).

Although Article 20 GDPR concerns the specific case of personal data it can in general contribute to the availability of data as, first, enforcing the portability right does not automatically lead to the deletion of the respective data (if this right is not exercised by the data subject cumulatively) but allows the transfer to various service providers and, second, a direct transfer of the data to another service provider can be claimed where technically feasible.[88] However, not the portability right itself but rather the necessary infrastructure, such as interoperable data formats, export and import tools, accessible interfaces and APIs have turned out to be the relevant problem of Article 20 GDPR in practice. The GDPR obliges the controller solely to provide the relevant personal data in a 'structured, commonly used and machine-readable format', but left it to the industry to develop effective means for facilitating data portability.[89] Since implementing the (technical) infrastructure

---

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

[85] Metzger, A., 'Access to and porting of data under contract law: Consumer protection rules and market-based principles', p. 295.

[86] See also Article 29 Data Protection Working Party, *Guidelines on the right to data portability*, WP 242 rev.01, pp. 9 et seq.

[87] Crémer, J., de Montjoye, Y. and Schweitzer, H., *Competition Policy for the digital era*, pp. 81 et seq.

[88] Drexl, J., 'Designing Competitive Markets for Industrial Data', *Journal of Intellectual Property, Information Technology and E-Commerce Law*, 2017, p. 286 paragraphs 155 et seq.; Graef, I., Husovec, M. and Purtova, N., 'Data Portability and Data Control: Lessons for an Emerging Concept in EU Law', *German Law Journal,* 2018, pp. 1369 et seq.

[89] To a certain extent (consumer protection perspective) Article 8 Unfair Commercial Practices Directive safeguards data portability in B2C relations as Article 9 (d) which specifies the term 'aggressive commercial practice' further, refers explicitly to 'onerous or disproportionate non-contractual barriers imposed by the trader where a consumer wishes to

for effective data portability in practice requires major investments, it has been observed that 'big players' – contrary to the initial objective of Article 20 GDPR – might potentially even benefit the most from this provision.[90]

According to Article 20 (4) GDPR, the portability right 'shall not adversely affect the rights and freedoms of others'.[91] Resultingly, the GDPR provides an internal instrument for resolving cases in which the data subject's portability right would conflict with potential trade secrets or intellectual property rights of the controller by means of a balancing of interest clause. While this provision already introduces sufficient flexibility for obtaining balanced results, the standards for the weighing of interests currently remain rather unclear.

Article 15 GDPR furthermore provides the data subject's right to access. However, Article 15 GDPR does not constitute an 'access right' in the strict sense. The data subject should rather be informed whether and which categories of personal data are processed for which purposes and enabled to verify if the personal data is processed lawfully. Even though Article 15 (3) contains the right to obtain a 'copy', access to individual-level datasets is not covered due to the different purpose of Article 15 and the specific provision of Article 20 GDPR.[92] Consequently, Article 15 GDPR – despite its title – does not play an important role for the context of data sharing but is primarily designed to safeguard the data subject's fundamental rights.

Generally, it has to be borne in mind that the GDPR applies not only in *B2C* relations but wherever personal data is at stake – i.e. to every processing of personal data in B2B, B2G and G2B relations – thus for sharing, using or granting access to personal data. While processing of personal data is necessarily to be governed by the GDPR in order to protect the data subject's fundamental rights and interests,[93] the blurred delineation between personal and non-personal data and, thus, the unclear scope of the GDPR contribute significantly to legal uncertainty in the context of data sharing.[94]

3.1.2. Regulation on the free flow of non-personal data: self-regulatory approach for B2B cloud service portability

One of the first regulatory steps towards a European data economy was the enactment of the Regulation on a framework for the free flow of non-personal data, which has the objective to

exercise rights under the contract, including rights to terminate a contract or to switch to another product or another trader'.

90 Crémer, J., de Montjoye, Y. and Schweitzer, H., *Competition Policy for the digital era*, p. 82. See for an empirical analysis recently Chen, C., Frey, C. and Presidente, G., *Privacy Regulation and Firm Performance: Estimating the GDPR Effect Globally*.

91 Cf. Recital 63 in regard to the parallel clause for the access right (Article 15 (4) GDPR); Article 29 Data Protection Working Party, *Guidelines on the right to data portability*, WP 242 rev.01, p. 12.

92 See recently European Data Protection Board, 'Guidelines 01/2022 on data subject rights – Right of access', p. 12.

93 Processing of personal data in the context of 'information society services' is regulated further by the ePrivacy Directive (2002/58/EC) which is planned to be replaced by the ePrivacy Regulation (the negotiation process is still ongoing, on 10 February 2021 Council Mandate for negotiations with European Parliament was adopted, see Doc. ST 6087 2021 INIT).

94 Furthermore, it has to be borne in mind that for sensitive personal data even stricter rules apply (see Article 9 GDPR). This is of particular importance as the definition of 'special categories of data' is currently subject of a request for a preliminary ruling from Austria potentially resulting in a broad definition of this concept, see Case C-446/21 (*Schrems III*).

facilitate the free movement of data within the EU.[95] As the Regulation's title clarifies, it applies solely to non-personal data. If datasets are composed of both personal and non-personal data, the Regulation only governs the non-personal data part, if personal and non-personal data within a dataset are inextricably linked, the entire dataset falls under the GDPR (Article 2 (2) Free Flow Regulation). Since data localisation requirements in national law had been identified as important obstacle to (cross-border) data sharing,[96] the Regulation has eliminated such data localisation requirements set forth in the Member States widely (unless they are justified on grounds of public security in compliance with the principle of proportionality, see Article 4 Free Flow Regulation).

In order to enhance the porting of data between cloud service providers for professional users, Article 6 of the Regulation implemented a self-regulatory approach. This provision stipulates the Commission's obligation to encourage and facilitate the development of codes of conduct for (cloud) service providers which should contain best practices, minimum information requirements and certification schemes. In December 2019, the first voluntary Codes of Conduct based on Article 6 of the Free Flow Regulation were presented by the working group on switching cloud providers and data porting ('SWIPO') for SaaS and IaaS cloud services.[97] The effective implementation of the Codes of Conduct, as required by Article 6 (3) of the Regulation, seem to have been only partially successful since until now only eight cloud service providers have submitted a declaration of adherence to a SWIPO Code of Conduct for IaaS and/or SaaS services. As the SWIPO codes have a strong focus on pre-contractual transparency obligations and remain rather abstract in regard to the relevant technical infrastructure, the self-regulatory approach appears insufficient to facilitate cloud service portability in B2B relations significantly. This corresponds with the stakeholders' answers to the Public Consultation on the Data Act in which 52 % of the respondents deem it necessary to establish a *right* to portability for business users of cloud computing services while 19 % are against such right.[98] According to 46 % of the respondents, implementing a portability right could be limited to high-level legal principles, whereas 29 % hold that more specific conditions of contractual, technical, commercial, and economic nature would be necessary. The Commission is currently evaluating these voluntary Codes of Conduct[99] and will provide further results concerning their impact by November 2022.[100] As this self-regulatory approach however 'seems not to have affected market dynamics significantly',[101] the proposal for a Data Act contains mandatory obligations for cloud and edge service providers in order to facilitate switching between different providers and porting data (see further below 4.5).

---

95 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.

96 Commission Staff Working Document, *On the free flow of data and emerging issues of the European data economy,* accompanying the document Communication Building a European data economy, SWD(2017) 2 final, 2017, pp. 5 et seq.; see also Everis Benelux, *Study on data sharing between companies in Europe*, pp. 27 et seq., 77.

97 https://digital-strategy.ec.europa.eu/en/news/presentation-codes-conduct-cloud-switching-and-data-portability. SWIPO Codes of Conduct, available at: https://swipo.eu/download-section/copyrighted-downloads/.

98 *Summary report on the Public Consultation on Data Act and Amended Rules on the Legal Protection of Databases*, Ref. Ares(2021)7509117, 2021, p. 5.

99 See European Commission, *Inception Impact Assessment Data Act*, Ref. Ares(2021)352715, 2021, p. 3.

100 See https://digital-strategy.ec.europa.eu/en/news/presentation-codes-conduct-cloud-switching-and-data-portability and Proposal of 23 February 2022 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 (hereinafter 'Data Act'), p. 9.

101 Proposal for a Data Act, p. 4, see also Recital 70 ('limited efficacy of the self-regulatory frameworks').

3.1.3. Open Data Directive: re-use of public sector information

In order to facilitate and regulate access to data held by the public sector (*G2B*) the Open Data Directive (replacing the PSI Directive[102]) was enacted in 2019.[103] The provisions, however, solely apply to data which is already accessible on the basis of existing European and national access regimes (Article 1 (3) Open Data Directive), new access rights as such are therefore not established.[104] The Directive rather aims at facilitating the re-use of public sector information held by public sector bodies or certain public undertakings and publicly funded research data for commercial or non-commercial purposes free of charge by providing a set of minimum rules governing the re-use and the practical arrangements for re-use. The Open Data Directive applies solely to *non-personal data*, see Article 1 (2) (h), and does not extend to documents protected by intellectual property rights of *third* parties (Article1 (2) (c)) or documents qualified as confidential information, see Article 1 (2) (d) Open Data Directive.[105] Where data affected by the provisions of the Open Data Directive is protected by the database sui generis right, according to Article 1 (6) Open Data Directive this right 'shall not be exercised by public sector bodies in order to prevent the re-use of documents or to restrict re-use beyond the limits set by this Directive'. The Open Data Directive covers also access to 'dynamic' data, thus to real-time data (see Article 5 (5), (6) and definition in Article 2 (8) Open Data Directive). Furthermore, specific conditions for so called high-value datasets (such as geospatial or meteorological data, data relating to earth observation and environment, statistics, companies and company ownership and mobility) are set forth in its Articles 13 et seq.

3.1.4. Sector specific-regulation

Due to identified market failures[106] certain sector-specific rules for data access, use and portability have been adopted, inter alia for

- the automotive sector (Regulation (EU) 2018/858),
- payment service providers (Payment Service Directive 2015/2366),
- smart metering information (Directive 2019/944 for electricity, Directive 2009/73/EC for gas meters),
- electricity network data (Regulation (EU) 2017/1485, Regulation (EU) 2015/703), and
- intelligent transport systems (Directive 2010/40/EU).[107]

---

[102] Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information (hereinafter 'PSI Directive').

[103] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information.

[104] Van Eechoud, M., 'A Serpent Eating Its Tail: The Database Directive Meets the Open Data Directive', *International Review of Intellectual Property and Competition Law*, 2021, p. 376.

[105] On the contrary, the proposed Data Governance Act as a complementary tool for enhancing access to public sector information is designed to cover personal data and data that is protected as confidential information or intellectual property (see below 3.1.6). The difficult distinction between personal and non-personal data (see below 3.3.3) is therefore also relevant for determining the applicability of the Open Data Directive or the Data Governance Act, see Richter, H., 'Ankunft im Post-Open-Data-Zeitalter', *Zeitschrift für Datenschutz*, 2021, p. 7.

[106] See explicitly European Commission, *A European strategy for data*, COM(2020) 66 final, 2020, p. 4.

[107] For a detailed description of some of these access rights see e. g. Graef, I., Husovec, M. and van den Boom, J., 'Spill-Overs in Data Governance: Uncovering the Uneasy Relationship Between the GDPR's Right to Data Portability and EU

3.1.5. Competition law

Apart from sector-specific regulation, access to data in B2B relation is primarily governed by general competition law under Article 102 TFEU (essential facilities doctrine) as the refusal to grant access to data might constitute an abuse of a dominant position.[108] According to the requirements originally developed in the *Magill* judgment for information protected by intellectual property rights, a competition law-based compulsory licence can be granted under the following conditions:[109] A rightholder with a market dominant position in regard to the licensing of the protected information refuses to licence the protected information (1) which is indispensable to compete in a downstream market, (2) without objective reason, (3) with the effect that any competition on that market is eliminated, and (4) thereby preventing the emergence of a new product or service for which there is a potential consumer demand.[110] The interpretation of these requirements has become more flexible over the years, in particular in regard to the aftermarket criterion indicating two different markets (upstream market and secondary downstream market) and to the notion of 'new product': In the first case, the CJEU clarified with its *IMS Health* judgment that the 'possibility of identifying a separate market', thus a mere hypothetical upstream licensing market, suffices.[111] In the second case, the definition of a new product was extended to situations where a refusal limits the technical development to the prejudice of consumers, hence to a product being at least more efficient but not necessarily 'new'.[112] The indispensability criterion is, however, understood quite restrictively and requires 'technical, legal or even economic obstacles capable of making it impossible, or even unreasonably difficult' to obtain the relevant information – thus being not economically viable for a competitor of comparable size and resources.[113] With the *Microsoft* judgment, the described requirements originally developed for intellectual property rights were also applied to information subject to trade secret protection.[114] Consequently, a compulsory licence based on Article 102 TFEU can on principle also justify access to trade secrets. As regards access to data, it has been proposed to adjust the criteria of the essential facilities doctrine by emphasising the underlying ratio of balancing the need for intervention by competition law carefully with the rightholder's freedom to contract and the risk of compromising its incentives to invest leading to reduced competition in the long term.[115]

Sector-Specific Data Access Regimes', *Journal of European Consumer and Market Law*, 2020, p. 3 et seq. Further specific regulation is provided in: Support Centre for data sharing, *Analytical report on EU law applicable to sharing of non-personal data*, pp. 11 et seq. and pp. 45 et seq.

[108] In regard to data access under competition law see comprehensively Crémer, J., de Montjoye, Y. and Schweitzer, H., *Competition Policy for the digital era*, pp. 91 et seq.

[109] CJEU, judgment of 6 April 1995, *RTE and ITP v Commission* (*Magill*), C-241/91 P and C-242/91 P, EU:C:1995:98.

[110] See also CJEU, judgment of 26 November 1998, *Bronner v Mediaprint*, C-7/97, EU:C:1998:569, paragraph 40; judgment of 29 April 2004, *IMS Health v NDC*, C-418/01, EU:C:2004:257, paragraphs 38, 48 et seq.

[111] CJEU, judgment of 29 April 2004, *IMS Health v NDC*, C-418/01, EU:C:2004:257, paragraphs 42 et seq. See further Leistner, M., 'Intellectual Property and Competition Law: The European Development from Magill to IMS Health Compared to Recent German and U.S. Case Law', *Zeitschrift für Wettbewerbsrecht*, 2005, pp. 150 et seq.

[112] Court of First Instance, judgment of 17 September 2007, *Microsoft v Commission*, T-201/04, EU:T:2007:289, paragraphs 643 et seq.

[113] CJEU, judgment of 26 November 1998, *Bronner v Mediaprint*, C-7/97, EU:C:1998:569, paragraphs 44 et seq.

[114] Court of First Instance, judgment of 17 September 2007, *Microsoft v Commission*, T-201/04, EU:T:2007:289, paragraph 289.

[115] Crémer, J., de Montjoye, Y. and Schweitzer, H., *Competition Policy for the digital era*, pp. 98 et seq. with reference to the argumentation of Advocate General Jacobs' Opinion 28 May 1998, *Bronner v Mediaprint*, C-7/97, EU:C:1998:264, paragraph 57.

In sum, general competition law can grant access to data by means of a compulsory licence based on Article 102 TFEU where the data holder has a dominant market position.[116] As far as the above-mentioned requirements are fulfilled in the respective case, access to individual-level data (first case group) in B2B relations is generally covered by Article 102 TFEU. Access to real-time data can be encompassed where it is 'indispensable'.[117] Despite the more flexible interpretation established in the *Microsoft* judgment, problems for the first case group might, however, arise in regard to the necessary separate aftermarket dominated by the data holder.[118] In the second case group, access to aggregated datasets in order to offer complementary or aftermarket service can be indispensable for competitors in particular cases, for instance in the context of machine-learning applications; thus, depending on the circumstances of the case, in theory Article 102 TFEU-based compulsory licences can be available if their conditions are met. Nevertheless, as regards the second case group, so far only few cases exist and there is still an ongoing debate on the adequate scope of the essential facilities doctrine (i.e. applicability to big data conglomerates).[119] The third case group concerning the access to large datasets for the development of unrelated products and services is, for the time being, not governed by competition law.[120]

3.1.6. Proposal for a Data Governance Act

The proposed Data Governance Act stipulates conditions for access to data held by the public sector and has a complementary role to the Open Data Directive. However, the Data Governance Act does not include access or use rights for such data. The Data Governance Act further aims at facilitating the handling of (personal) data for altruistic purposes and through data intermediaries by providing a legal framework for respective services. As data intermediaries and data trustees could possibly play an important role in a European data economy – both in B2C and B2B relations[121] – the proposed provisions are designed to establish a solid basis for their development. Fostering the development of data intermediaries and respective services corresponds also with the Commission's objective to create sector-specific and personal common European data spaces as defined in the Data Strategy.[122]

---

[116] For the difficulties of defining markets and market power in the data economy see comprehensively Crémer, J., de Montjoye, Y. and Schweitzer, H., *Competition Policy for the digital era*, pp. 42 et seq. The German Act Against Restraints of Competition (GWB) goes further as the provisions on abuse of market power apply also to undertakings with 'relative market power', thus in cases in which undertakings are dependent on another undertaking in such a way that sufficient and reasonable possibilities for switching to third parties do not exist, see Sec. 20 (1). Recently there has been introduced a new Sec. 20 (1a) stating that 'relative market power' may also arise from the fact that an undertaking is dependent on accessing data controlled by another undertaking in order to carry out its own activities.

[117] Crémer, J., de Montjoye, Y. and Schweitzer, H., *Competition Policy for the digital era*, pp. 101 et seq.

[118] Crémer, J., de Montjoye, Y. and Schweitzer, H., *Competition Policy for the digital era*, pp. 101 et seq. As a consequence, a particular provision for abusive conduct of 'undertakings of paramount significance for competition across markets' has been introduced in Sec. 19a of the German Act Against Restraints of Competition (GWB) which allows sanctioning by the German Federal Cartel Authority (Bundeskartellamt).

[119] Schweitzer, H. and Welker, R., 'A legal framework for access to data – A competition policy perspective', pp. 141 et seq.; Crémer, J., de Montjoye, Y. and Schweitzer, H., *Competition Policy for the digital era*, pp. 102 et seq.

[120] Schweitzer, H. and Welker, R., 'A legal framework for access to data – A competition policy perspective', pp. 145 et seq.

[121] Picht, P. and Richter, H., *The Proposed EU Digital Services Regulation 2020: Data Desiderata*, pp. 9 et seq.; Martens, B. and others, *Business to business data sharing: an economic and legal analysis*, pp. 28; Schweitzer, H. and Welker, R., 'A legal framework for access to data – A competition policy perspective', pp. 142 et seq.

[122] European Commission, *A European strategy for data*, COM(2020) 66 final, 2020, p. 12 et seq.

Notably, the Data Governance Act already contains provisions in regard to the relation between access rights and intellectual property rights/trade secrets. Where access to public sector data protected by intellectual property rights is granted, the conditions for *re-use* should be governed by the respective right (see Article 5 (7) Data Governance Act). However, the sui generis database right 'shall not be exercised by public sector bodies in order to prevent the re-use of data or to restrict re-use beyond the limits set by this Regulation'. The sui generis right as most relevant intellectual property right for protecting collections of data is, therefore, in principle ruled out. As regards access to confidential information, according to Article 5 (8) Data Governance Act their re-use must at least not lead to the disclosure of the secret information. However, it remains quiet on other types of downstream uses.

3.1.7. Proposal for a Digital Markets Act

Taking up aspects also discussed in the context of the portability right in Article 20 GDPR, the proposal for a Digital Markets Act[123] provides end users and, according to the original proposal, also business users of gatekeeper platforms with a right to portability (Article 6 (h)) of data they provided or generated in the context of their use, i.e. volunteered and observed data (Recital 54), comprising continuous and real-time access, and the implementation of effective tools for exercising the portability right. Furthermore, Article 6 (i) Digital Markets Act adds an access right for business platform users (and third parties authorised by a business user acting as processor) free of charge, with effective, high-quality, continuous and real-time access, according to the original proposal including inferred data from such use (see Recital 55), in aggregated or non-aggregated form. These two rights relate to the first case group, namely to individual use data or co-generated data and are (currently) designed without remuneration. As regards horizontal access to aggregated datasets (second case group), Article 6 (j) Digital Markets Act foresees a specific access right for third party providers of online search engines to ranking, query, click and view data of gatekeepers under FRAND terms. This latter right is particularly remarkable not only because it concerns aggregated data but also because it applies in favour of market participants which might be in direct competition with gatekeeper search engines.

According to the Commission's proposal, the Digital Markets Act does explicitly not qualify as competition law but should complement the existing national and EU competition rules.[124] Consequently, Article 114 TFEU (establishment and functioning of the internal market) serves as legal basis for the proposed Digital Markets Act. However, due to its objectives and its instruments, the Digital Markets Act notably shows elements of competition law.[125] While on the one hand the Digital Markets Act shall be without prejudice to (the stricter standards in) EU and national competition law, Article 1 (6), on the other hand, the Member States should neither impose further obligations on gatekeepers (Article 1 (5)), nor should national authorities adopt decisions which would contradict those taken by the Commission (Article 1 (7) Digital Markets Act). Without

[123] On 25 March 2022 the Council and the Parliament have reached a provisional political agreement on the Digital Markets Act. As the formal approval of the text is still ongoing we refer to the original Commission's proposal of 15 December 2020, COM(2020) 842 final.

[124] Proposal for a Digital Markets Act, COM(2020) 842 final, 2020, p. 3, Recitals 9 and 10.

[125] Leistner, M., 'The Commission's vision for Europe's digital future: proposals for the Data Governance Act, the Digital Markets Act and the Digital Services Act – a critical primer', *Journal of Intellectual Property Law & Practice*, 2021, p. 779 et seq.

clarifying the relation to competition law and without cooperation between the competent (national and European) authorities, this would result in overlapping, unharmonised – and thus, inefficient – (public) enforcement activities.[126] Not only to highlight the Digital Markets Act's pro-competitive character but also for opening the possibility to make use of the established structures of competition law enforcement which includes the cooperation within the 'European Competition Network', Article 103 TFEU should be used as additional legal basis.[127]

As a result, the proposed Digital Markets Act regulates the conditions for access and portability of data but does – contrary to competition law – not cover the conditions for re-use of the respective data. Therefore, the conditions for re-use of accessible and portable data would be governed by intellectual property and trade secrets law (or potentially by general competition law[128]). In contrast to the Data Governance Act, the Digital Markets Act, for the time being, does not include provisions on the relation to trade secret protection and intellectual property rights.

3.1.8. Contract law

a. Individual-level use data

Concerning *B2C relationships*, Article 16 (4) Digital Content Directive[129] provides for a portability right of the consumer after contract termination. This provision relates solely to non-personal data which was provided or created by the consumer during the use of the digital content or digital service.[130] Irrespective of any contract law provision, consumers as 'data subjects' are always entitled to exercise their individual rights set forth in the GDPR in regard to their personal data (see above 3.1.1).

For *B2B relationships* so far European contract law does not establish a general right to access, use or portability of individual-level use data. Consequently, under the contract law's current framework business users of digital services (including cloud services) or platforms are not entitled to access or port data neither during the use of a service nor after the termination of contract by default.[131] Rather, the parties have to agree on access, portability, and use rights by means of contract. [132]

---

[126] Leistner, M., 'The Commission's vision for Europe's digital future: proposals for the Data Governance Act, the Digital Markets Act and the Digital Services Act – a critical primer', *Journal of Intellectual Property Law & Practice*, 2021, p. 779 et seq.

[127] Leistner, M., 'The Commission's vision for Europe's digital future: proposals for the Data Governance Act, the Digital Markets Act and the Digital Services Act – a critical primer', *Journal of Intellectual Property Law & Practice*, 2021, p. 781.

[128] An important question to solve is the relation between the DMA and competition law as according to its Article 1 (6) the DMA on the one hand should be without prejudice to competition law, on the other hand national authorities are required not to take decisions inconsistent with those of the Commission.

[129] Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services (hereinafter 'Digital Content Directive').

[130] See further in this regard Metzger, A., 'Access to and porting of data under contract law: Consumer protection rules and market-based principles', pp. 290 et seq.

[131] Metzger, A., 'Access to and porting of data under contract law: Consumer protection rules and market-based principles', pp. 290 et seq. However, it is discussed if access rights could be established based on non-mandatory principles such as the Principles of European Contract Law (PECL), the Unidroit Principles or the Draft Common Frame of Reference (DCFR), see ibid.

[132] See in regard to portability rights Commission Staff Working Document, *On the free flow of data and emerging issues of the European data economy,* accompanying the document Communication Building a European data economy, SWD(2017) 2 final, 2017, p. 47.

Even though not genuine contract law, the *Platform to Business Regulation*[133] comes into play as it stipulates certain transparency obligations for platforms in relation to their business users: According to Article 9 P2B Regulation, the platform provider inter alia has to include in its terms and conditions information about contractual and technical access to data provided by the user and data generated through the provision of the service. Only for the very specific case of restriction, suspension or termination by the service provider Article 4 (3) P2B Regulation sets forth a data access right for the business user. In sum, the P2B Regulation establishes a transparency framework for business users of platform services – which in certain aspects is planned to be extended in a more general way through the proposal for a Digital Services Act (see e.g. transparency obligations in its Articles 12 et seq.).[134]

b. Horizontal data sharing

Horizontal data sharing is primarily based on contract law. While the existing contract law framework in general provides a comprehensive basis for agreements on data sharing as such, well-established guidelines for data licensing contracts are currently lacking. The Commission meanwhile has provided certain soft law instruments, i.e. best practices for B2B and B2G data sharing on contractual basis.[135] However, these guidelines and principles remain rather abstract and of a general nature suggesting inter alia to define what data shall be made available, who can access and (re-)use the data, what the (re-)user can do or what data need to be protected and how.[136]

Recently, the development of comparable best practices and soft law instruments can be observed internationally and by very different actors (see for instance comparable guidelines of the Japanese Ministry of Economy, Trade and Industry,[137] the ALI-ELI principles for a data economy,[138] initiatives like the Montreal Data License[139] or data use agreements of several service providers, e.g. Microsoft).[140] Furthermore, certain sector specific initiatives, such as in the agricultural sector, already have led to results such as the 'Code of conduct on agricultural data sharing by contractual agreement'.[141] Remarkably this Code of conduct clearly assigns agricultural data to the 'data

---

[133] Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services (hereinafter 'P2B Regulation').

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

[135] European Commission, *Towards a common European data spac*e, COM(2018) 232 final, 2018, accompanied by the more detailed Staff Working Document, *Guidance on sharing private sector data in the European data economy*, SWD/2018/125 final, 2018.

[136] See also Metzger, A., 'Access to and porting of data under contract law: Consumer protection rules and market-based principles', p. 311.

[137] Ministry of Economy, Trade and Industry (METI), *Contract Guidelines on Utilization of AI and Data*, Version 1.1..

[138] *ALI-ELI Principles for a Data Economy – Data Transactions and Data Rights*, ELI Final Council Draft, 2021.

[139] See Benjamin, M., Gagnon. P. and other, 'Towards Standardization of Data Licenses: The Montreal Data License', *ArXiv*, abs/1903.12262, 2019.

[140] See at: https://news.microsoft.com/opendata/. See for an overview of existing model contract terms, also sector-specific ones, Support Centre for data sharing, *Report on collected model contract terms*.

[141] EU Code of conduct on agricultural data sharing by contractual agreement, 2018 (available at: https://www.scc-gmbh.de/images/scc/Downloads/EU_Code_of_conduct_on_agricultural_data.pdf). See in this regard also Schweitzer, H. and Welker, R., 'A legal framework for access to data – A competition policy perspective', p. 131; Atik, C. and Martens, B., 'Competition Problems and Governance of Non-personal Agricultural Machine Data: Comparing Voluntary Initiatives in the US and EU', *Journal of Intellectual Property, Information Technology and E-Commerce Law*, 2021, pp. 370 et seq. Similar Codes of Conduct for the agricultural sector exist in the US, New Zealand and Australia,

originator' who may 'permit' the collection, access and use of the data by means of contractual agreement (see further below).

In regard of facilitating access to data held by private companies by public bodies (*B2G*), the Commission has appointed a High-Level Expert Group on Business-to-Government Data Sharing which presented its final report in 2020.[142] This report names eight key principles for B2G data sharing, namely proportionality, purpose limitation, protection of legitimate interests (e. g. trade secrets), mutual beneficial contract conditions for data re-use, mitigation of limitations of private sector data, transparency and societal participation, accountability of all partners and the commitment to fair, and ethical data use.

3.1.9. Summary

The existing legal framework leads to the following results which will be categorised based on the above defined case groups (see 2.1.5) in which data access, use and portability rights are conceivable:

Access and portability of *individual-level use data* (*first case group*) is provided for voluntary and observed personal data through Article 20 GDPR. In the context of B2C contracts for the supply of digital content or digital services voluntary and observed non-personal data have to be provided after contract termination, Article 16 (4) Digital Content Directive. Furthermore, certain sector-specific regulation relates to the access of individual-level use data (e.g. Directive 2019/944 in context of electricity/smart meters and Payment Service Directive 2015/2366[143]). For business users so far no general data access or portability right – unless of course foreseen in respective contractual agreements – exists. However, an important extension of access and portability rights for individual use data can be expected with the proposed Digital Markets Act for both individual and business users in relation to gatekeeper platforms designed to cover also real-time data and (potentially) inferred data. Apart from that, access to co-generated data is currently not granted in relation to service providers other than gatekeepers. General competition law, namely Article 102 TFEU, may apply where refusing access to data amounts to an abuse of a dominant position. As regards cloud service portability for business users, the Regulation on the free flow of non-personal data has attempted to encourage the development of Codes of Conduct, however this self-regulatory approach by now has not led to effective portability in practice.

Horizontal data access of competitors to complete sets of aggregated data necessary for workable competition in aftermarkets or complementary markets (*second case group*) is primarily governed by general competition law and a few sector-specific provisions (for instance Regulation (EU) 2018/858 in regard to vehicle repair and maintenance information). The proposed Digital Markets Act addresses this case group and also the issue of access to large aggregated datasets for innovation purposes (*third case group*), albeit solely for the specific case of search engine providers which have the right to access under FRAND conditions in relation to gatekeepers.

---

see e.g. van der Burg, S., Wiseman, L. and Krkeljas, J., 'Trust in farm data sharing: reflections on the EU code of conduct for agricultural data sharing', *Ethics and Information Technology*, 2021, p. 186.

[142] High-Level Expert Group on Business-to-Government Data Sharing, *Towards a European strategy on business-to-government data sharing for the public interest*.

[143] See further Schweitzer, H. and Welker, R., 'A legal framework for access to data – A competition policy perspective', pp. 120 et seq.

The conditions for access and re-use of *public sector information* (*fourth case group*) are regulated by the Open Data Directive and planned to be complemented by the proposed Data Governance Act. These legal instruments, however, set out conditions for access and re-use and do not establish rights to access or re-use.

3.2. Intellectual property rights and their impact on data access, portability and re-use

Intellectual property law and trade secret protection do not come into play as instruments to grant access and portability rights but concern in particular the subsequent conditions for the (re-)use of data protected by these instruments. In addition, the provisions of the Computer Programs Directive play an important role for providing the necessary technical infrastructure for data sharing in regard to data formats and APIs while general copyright law and its exceptions for text and data mining have to be considered for the collection and aggregation of data.

3.2.1. Computer Programs Directive: interoperability and interfaces

Essential basis for data sharing and the portability of data is the technical infrastructure for data flows, particularly free and accessible APIs and interoperable data formats. In this context the Computer Programs Directive[144] can generally become relevant as far as the copyright protection of computer programs would extend to interface structures (particularly interface specifications) and/or data formats.

The Computer Programs Directive protects all forms of expression of a computer program capable of leading to the reproduction of such program (Article 1 (2) of the Directive), hence source code and object code of a computer program.[145] Article 1 (2) of the Directive expressly codifies the general idea-expression-dichotomy for the specific area of computer programs stating that 'ideas and principles which underlie any element of a computer program, including those which underlie its interfaces, are not protected by copyright under this Directive.' Based on these two core principles delineating the Computer Programs Directive's scope, the CJEU decided that data file formats and programming languages as such may not qualify for protection.[146] Due to Article 1 (2) of the Directive, at least interface specifications are therefore not protected through copyright. Based on the CJEU's judgment in *SAS*, however, it is argued that interfaces as such – potentially including their concrete 'expression' in code form – should not be covered by copyright protection either.[147] As

[144] Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs (hereinafter 'Computer Programs Directive').

[145] CJEU, judgment of 22 December 2010, *BSA v Ministry of Culture*, C-393/09, EU:C:2010:816, paragraphs 34 et seq.

[146] CJEU, judgment of 2 May 2012, *SAS Institute v WPL*, C-406/10, EU:C:2012:259, paragraphs 29 et seq.

[147] Marly, J., 'Der Schutzgegenstand des urheberrechtlichen Softwareschutzes', *Gewerblicher Rechtsschutz und Urheberrecht*, 2012, p. 779; more tentative Vezzoso, S., 'Copyright, Interfaces, and a Possible Atlantic Divide', *Journal of Intellectual Property, Information Technology and E- Commerce Law*, 2012, p. 153, paragraph 40; Samuelson, P., Vinje, T. and Cornish, W., 'Does copyright protection under the EU Software Directive extend to computer program behaviour, languages and interfaces?', *European Intellectual Property Review,* 2012, pp. 158–159, 163–164; cf. Heinze, C., 'Software als Schutzgegenstand des Europäischen Urheberrechts', *Journal of Intellectual Property, Information Technology and E-Commerce Law,* 2011, p. 97, paragraph 8.

regards US copyright, the Supreme Court has shown at least a tentative approach for protecting programming interfaces under copyright law in the *Google v Oracle* case.[148]

Furthermore, the Computer Programs Directive stresses the importance of interoperability as one of its main regulatory objectives (see e. g. Recitals 10, 11, 15, 17). This is supported by the mandatory provision of Article 6 Computer Programs Directive which allows for the decomplication of computer programs where it is indispensable to obtain information necessary to achieve interoperability.[149] However, the importance of this provision remains limited as first, the requirements are very high, and second, factual limits – such as trade secret protection or secrecy – constitute an obstacle for the accessibility of program code in general. Put in a more general way, in regard to computer programs certain problems of de facto control over code, including interface structures, can be observed.

Nevertheless, the Computer Programs Directive itself provides sufficient flexibility for dealing with the needs of a data-driven economy which was even manifested further by the CJEU's specification of its scope.

3.2.2. Database Directive: potential obstacle to data access, re-use and portability?

The Database Directive provides protection for databases with a two-fold system, first, through copyright (Articles 3 et seq.) and, second, through the sui generis right for the database maker (Articles 7 et seq.). While copyright protects an author's own intellectual creation expressed in the selection or arrangement of the database's content, the sui generis right enables the database maker to prevent any extraction and/or re-utilisation of the database's content where there has been a substantial investment in obtaining, verification or presentation of these contents. Three main objectives of the Database Directive can be identified consisting in harmonising the database protection in the EU (Recitals 1–4), safeguarding and thereby promoting the investment in the production of databases (cf. Recitals 10–12) and balancing the interests of database makers and database users (e.g. Recital 49).[150]

Since the enactment of the Database Directive in 1996, the creation of databases and their contents have changed significantly from 'the manual gathering of existing data, over automatic processes of data collection, even to automatic creation of data (e.g. sensor-generated data)'.[151] IoT has led to a far-reaching equipment of products, devices or machines with sensors observing or generating data. Big data analytics allow not only the observation and analysis but also the combination of huge amounts of data from different sources and cloud computing provides the infrastructure for storing data once collected over long time periods. As a result, the variety of available data from multiple

---

[148] U.S. Supreme Court, judgment of 5 May 2021, *Google LLC v. Oracle America INC,* No. 18-956. The Supreme Court left the question of a copyrightability of interfaces open as it argued that in any case a fair use was given.

[149] See for instance CJEU, judgment of 6 October 2021, *Top System v Belgian State*, C-13/20, EU:C:2021:811, paragraphs 44 et seq.

[150] DG Internal Market and Services Working Paper, *First evaluation of Directive 96/9/EC on the legal protection of databases*, 2005, p. 3; Bently, L., Derclaye, E. and others, *Study in support of the evaluation of Directive 96/9/EC on the legal protection of databases*, p. ii.

[151] Bently, L., Derclaye, E. and others, *Study in support of the evaluation of Directive 96/9/EC on the legal protection of databases*, p. 26.

sources and the automatisation of data processing also affect the collection of information and, thus, the creation of databases.[152]

Due to these major changes to the data ecology, the Database Directive was subject to an evaluation twice, in 2005[153] and 2018[154]. Both evaluations brought up that the Directive was indeed effective as regards the harmonisation of database protection in the EU, but no evidence could be found that the sui generis right has been effective in stimulating the investment in databases and in establishing a functioning access regime.[155] Even though in 2005 and 2018 significant changes to the Directive and different policy options (including the withdrawal of the sui generis right)[156] were discussed and proposed, this did not lead to major amendments of the Database Directive.[157]

For both, copyright protection and sui generis right, the term 'database' refers to any collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means (Article 1 (2) Database Directive.). With reference to the sui generis right's function, the CJEU interprets the term database and the requirement of 'independent materials' very broadly.[158] In the decision *Freistaat Bayern v Verlag Esterbauer*, the CJEU classified even individual geographical information extracted from a topographic map which can be used to produce and market another map as 'independent materials' – and therefore a map as 'database' in the sense of Article 1(2) Database Directive.[159] Consequently, the majority of datasets in the context of big data analytics could generally qualify as databases, potentially including even dynamic, real-time datasets and any non-relational databases.[160]

a. Copyright protection for database works

According to Article 3 (1) Database Directive, databases can be protected by copyright if the collection or arrangement of their contents constitute the author's own intellectual creation. Over

---

[152] See further Bently, L., Derclaye, E. and others, *Study in support of the evaluation of Directive 96/9/EC on the legal protection of databases*, pp. 26 et seq. with empirical results.

[153] DG Internal Market and Services Working Paper, *First evaluation of Directive 96/9/EC on the legal protection of databases*, 2005. See in this regard Kur, A., and others, 'First Evaluation of Directive 96/9/EC on the Legal Protection of Databases – Comment by the Max Planck Institute for Intellectual Property, Competition and Tax Law, Munich', *International Review of Intellectual Property and Competition Law,* 2006, pp. 551 et seq.

[154] Commission Staff Working Document, *Evaluation of Directive 96/9/EC on the legal protection of databases*, SWD(2018) 146 final, 2018, which was supported by Bently, L., Derclaye, E. and others, *Study in support of the evaluation of Directive 96/9/EC on the legal protection of databases*.

[155] Commission Staff Working Document, *Evaluation of Directive 96/9/EC on the legal protection of databases*, SWD(2018) 146 final, 2018, p. 46; similarly DG Internal Market and Services Working Paper, *First evaluation of Directive 96/9/EC on the legal protection of databases*, 2005, pp. 24 et seq.

[156] DG Internal Market and Services Working Paper, *First evaluation of Directive 96/9/EC on the legal protection of databases*, 2005, pp. 25 et seq.; Bently, L., Derclaye, E. and others, *Study in support of the evaluation of Directive 96/9/EC on the legal protection of databases*, pp. 140 et seq.

[157] Commission Staff Working Document, *Evaluation of Directive 96/9/EC on the legal protection of databases*, SWD(2018) 146 final, 2018, p. 47, pointing at the 'restricted policy potential' and 'the limited range of problems' which would make an reform 'largely disproportionate'.

[158] See explicitly CJEU, judgment of 29 October 2015, *Freistaat Bayern v Verlag Esterbauer*, C-490/14, EU:C:2015:735, paragraphs 12 et seq.

[159] CJEU, judgment of 29 October 2015, *Freistaat Bayern v Verlag Esterbauer*, C-490/14, EU:C:2015:735, paragraphs 18 et seq.

[160] Drexl, J., *Data Access and Control in the Era of Connected Devices – Study on Behalf of the European Consumer Organisation BEUC,* 2018, pp. 73–76.

the last years, the CJEU defined the threshold for an own intellectual creation more and more precisely, thus establishing a sound European concept of 'work'.[161] According to the CJEU's decision *Football Dataco*, a database can be protected as an own intellectual creation 'when, through the selection or arrangement of the data which it contains, its author expresses his creative ability in an original manner by making free and creative choices (...) and thus stamps his 'personal touch''.[162] Where technical or mathematical considerations, rules or methods, however, leave no room for such creative decisions a database does not qualify for copyright protection. The CJEU highlighted its generally strict understanding of the notion 'creative choice' in the context of the copyrightability of military status reports stating that an expression determined solely by the information it contains and thus characterised by its technical function does not suffice for an own intellectual creation.[163] Since 'originality' in this sense under European law is the only relevant criterion for copyright protection (see also Recital 16 Database Directive), mere intellectual effort, skill, judgment, and labour in the collection or arrangement of the database's elements cannot lead to copyright protection.[164]

Article 3 Database Directive clearly states that solely the collection and arrangement of the content – hence a database's structure and not its content itself – are subject to copyright protection. In the context of AI and big data the selection and combination of training data, structuring and weighing of cost functions or systematic structures which form basis for generating inferred data could generally qualify as 'creative' compilation of independent elements. However, due to the rather high requirements for an own intellectual creation which also have to be applied to database works only an outstanding selection and combination of data (e.g. specific training datasets) could be protected under copyright law. In contrast, typical compilations of data which aim at optimising training datasets or the weighing of cost functions' parameters are characterised by certain technical or mathematical considerations and will therefore not fulfil the originality threshold. Copyright protection for database works will, therefore, generally play only a very marginal role, or at least, not raise intricate problems hampering data access, re-use and data sharing since the definition of 'work' will prevent an unadjusted extension of copyright protection.

b. Database sui generis right

i. Scope and conditions of protection

Contrary to the copyright protection of databases, the sui generis right has the potential to play a crucial role for the European data economy and for the envisaged objective of fostering data sharing, access and re-use as its scope of protection may potentially cover many typical big data and AI scenarios.[165] The impact of the database sui generis right is further intensified by its term of protection of fifteen years after a database's completion (see Article 10 (1) Database Directive).

---

[161] See most recently CJEU, judgment of 11 June 2020, *Brompton v Get2Get*, C-833/18, EU:C:2020:461, paragraphs 22 et seq.

[162] CJEU, judgment of 1 March 2012, *Football Dataco v Yahoo*, C-604/10, EU:C:2012:115, paragraph 38.

[163] CJEU, judgment of 29 July 2019, *Funke Medien v Germany*, C-469/17, EU:C:2019:623, paragraph 24.

[164] CJEU, judgment of 1 March 2012, *Football Dataco v Yahoo*, C-604/10, EU:C:2012:115, paragraphs 40 et seq.

[165] Leistner, M., 'Big Data and the EU Database Directive 96/9/EC: Current Law and Potential for Reform', pp. 27 et seq.; Leistner, M., 'The existing European IP rights system and the data economy', pp. 226 et seq.; Drexl, J., *Data Access and Control in the Era of Connected Devices*, pp. 67–85. More tentative Bently, L., Derclaye, E. and others, *Study in support of the evaluation of Directive 96/9/EC on the legal protection of databases*, pp. 29–31.

However, such an extensive term of protection is disproportionate for machine-generated data in particular and the dynamic developments in a data-driven economy in general (see further below, 3.3.1.a.iii).

According to Article 7 (1) Database Directive, the sui generis right applies to databases if there has been a qualitatively and/or quantitatively substantial investment in either the obtaining, verification or presentation of the contents. Due to the broad scope of the sui generis right, it can in practice come close to an exclusive property right against the use of data as such:[166] In cases in which data is solely available from one particular source, for instance because the data is created or made up by the respective database maker and, thus, cannot be obtained with comparable investments otherwise ('sole source situation'), the sui generis right factually would amount to a protection of the generated data, going way beyond its objective to protect the database marker's *investment*.

As a consequence, the CJEU since its landmark decisions *British Horseracing Board* and *Fixture Marketing* limits the scope of the sui generis right by excluding investments in the mere creation or generation of data as this often would result in the described 'sole source databases'.[167] In regard to the diverse data collection scenarios in a data-driven economy it is, however, not always possible to draw a clear line between the *collection* and the mere *creation* of data. Already the Commission's evaluation in 2018 stated: '[I]n the context of automated data collection by sensor-equipped, connected 'Internet of Things' objects, it becomes increasingly difficult to distinguish between data creation and obtaining of data when there is systematic categorisation of data already by the data-collecting object (e.g. industrial robots). Also, business models are changing as a result of digitisation and the economic importance of what today may appear to be a by-product of a physical process (data generation) may be at the core of the significant business model of tomorrow.'[168] However, the Commission at the same time has derived thereof, that 'the sui generis right does not apply to databases that are the by-products of the main activity of an organisation' meaning 'that the sui generis right does not apply broadly to the data economy (machine-generated data, IoT devices, big data, AI, etc.).'[169] Along these lines, some authors came to the conclusion that the majority of machine-generated data would fall outside the scope of the sui generis right.[170]

National courts, however, have deemed investments in establishing the necessary technical infrastructure for measuring, obtaining or documenting data, e.g. by equipping machines with sensors, as relevant investment in the collection of data.[171] Due to the diverging interpretation in

---

166 See already DG Internal Market and Services Working Paper, *First evaluation of Directive 96/9/EC on the legal protection of databases*, 2005, p. 24.

167 CJEU, judgment of 9 November 2004, *British Horseracing Board v Hill*, C-203/02, EU:C:2004:695, paragraphs 30 et seq. CJEU, judgments of 9 November 2004, *Fixtures Marketing v Oy Veikkaus,* C-46/02, EU:C:2004:694; *Fixtures Marketing v Svenska Spel,* C-338/02, EU:C:2004:696; *Fixtures Marketing v Organismos prognostikon,* C-444/02, EC:C:2004:697.

168 Commission Staff Working Document, *Evaluation of Directive 96/9/EC on the legal protection of databases*, SWD(2018) 146 final, 2018, p. 36.

169 Commission Staff Working Document, *Executive Summary of the Evaluation of Directive 96/9/EC on the legal protection of databases*, SWD(2018) 147 final, 2018, p. 2.

170 See also Bently, L., Derclaye, E. and others, *Study in support of the evaluation of Directive 96/9/EC on the legal protection of databases*, p. 20: 'most machine-generated data should remain out of the scope of the sui generis right, though it is not always clear whether the data is generated (created) rather than obtained (collected)'.

171 German Federal Supreme Court (BGH), judgment of 21 July 2005, *HIT Bilanz*, I ZR 290/02; cf. German Federal Supreme Court (BGH), judgment of 25 March 2010, *Autbahnmaut*, I ZR 47/08; Austrian Federal Supreme Court (OGH), judgment of 24 March 2015, 4 Ob 206/14; see in this regard also Leistner, M., 'Big Data and the EU Database Directive 96/9/EC: Current Law and Potential for Reform', pp. 28 et seq.; Bently, L., Derclaye, E. and others, *Study in support of the evaluation*

the Member States and as the CJEU so far has not explicitly[172] decided on a comparable question, significant fragmentation and legal uncertainty exist with respect to the distinction between creation and collection where machine-generated data is concerned intensifying the sui generis right's potential to hamper (necessary) access to data.

As the CJEU's jurisdiction can be interpreted as allowing for a functional, competition-oriented approach, a potential way out would be looking at the *function* and the *purpose* of the sui generis right instead of applying a merely formalistic distinction.[173] Following such competition-oriented distinction, classical sole source database situations in which data is (in the context of another main activity) created by the manufacturer would be qualified as *irrelevant creation* of data while measuring data through sensors could in general amount to a *relevant collection* of independently existing data.[174] Applying this standard, sole source databases would be excluded from protection in any case and regardless of their qualification as volunteered or observed data. For sensor-generated data it has to be distinguished further: If sensor-equipped machines collect or measure external data (e.g. outside temperature, location data) which are available from different sources, this would qualify as relevant data collection. However, the essential requirement would be the realistic possibility for competitors to collect the relevant data themselves, e.g. where machines are equipped with standardised sensors. On the contrary, machine internal (real-time) operational data would tend to be excluded as irrelevant data creation because the collection of such data cannot be separated from running the machine as such and the measured information cannot realistically be obtained by external sensors. Inferred data and particularly structured training data would potentially fall outside the sui generis right's scope as they would not amount to a collection of *independently existing* data insofar as the underlying volunteered or observed data are not available for other competitors.

When looking, for instance, at sensor-generated vehicle data, measuring the outside temperature is carried out by a standardised sensor so that respective data might be obtained also from other manufacturers. Consequently, the documentation of the outside temperature would qualify as relevant *collection* of data and, thus, fall under the sui generis right. However, measuring the cylinder or oil temperature for purposes of smart maintenance cannot be separated from driving the car and neither be obtained by competitors via external sensors leading to a mere *creation* of data. Consequently, and rightly so, the sui generis right does not apply as this constitutes a classical sole source situation. As a result, the already above-mentioned Regulation (EU) 2018/858 obliges vehicle manufacturers to provide unrestricted, standardised and non-discriminatory access to vehicle repair and maintenance information (as well as to the necessary tools) to independent operators (see its Article 61). While the proposed competition-oriented distinction between collection and generation could provide a reasonable standard for defining the sui generis right's scope in regard to machine-

of Directive 96/9/EC on the legal protection of databases, pp. 111 et seq.; Drexl, J., *Data Access and Control in the Era of Connected Devices*, pp. 72 et seq.

[172] The *Freistaat Bayern v Verlag Esterbauer* judgment (CJEU, 29 October 2015, C-490/14, EU:C:2015:735) might however be interpreted as expressing a similar tendency, see Leistner, M., 'Big Data and the EU Database Directive 96/9/EC: Current Law and Potential for Reform', p. 29.

[173] Leistner, M., 'The existing European IP rights system and the data economy', pp. 226 et seq.; see also Drexl, J., *Data Access and Control in the Era of Connected Devices,* pp. 68, 71–73.

[174] German Federal Supreme Court (BGH), judgment of 21 July 2005, *HIT Bilanz*, I ZR 290/02; cf. German Federal Supreme Court (BGH), judgment of 25 March 2010, *Autobahnmaut*, I ZR 47/08 and further Leistner, M., 'Big Data and the EU Database Directive 96/9/EC: Current Law and Potential for Reform', pp. 28 et seq.; Leistner, M., Antoine, L. and Sagstetter, T., *Big Data,* pp. 65 et seq., p. 450.

generated data, it remains unclear whether the courts would rely on comparable standards and case groups.

In sum, due to the vague definition of the sui generis right's scope, currently, there is significant legal uncertainty if and under which circumstances volunteered and observed data (in particular machine-generated data) could qualify as relevant collection of data and hence for protection. Inferred data seem to amount to an irrelevant creation, thus not provoking significant problems. Therefore, it seems necessary to specify the scope of the sui generis right further, for instance by clarifying the collection vs. generation distinction and providing for a catalogue of certain non-conclusive exemplary case groups.[175]

Second condition for the protection of a database under the sui generis right is a *substantial* investment.[176] The substantiality threshold is in general interpreted broadly and often even understood as mere 'de minimis exclusion'.[177] Due to a lack of specific interpretative guidelines by the CJEU , the requirement of substantial investment is treated differently in the Member States.[178] As a result of interpreting the substantiality standard extensively, the majority of relevant investments in the context of data-driven business models will qualify as substantial investment.[179]

ii. Exclusive rights and scope of protection

According to Article 7 (1) of the Database Directive, the database maker can prevent any extraction or re-utilisation of the whole database or a substantial part of the contents of that database. The CJEU defines these terms very broadly. For instance, the exclusive rights include an indirect extraction or cases where the extraction leads to a substantially changed and even value-added database.[180] In addition, business models as meta search engines may generally amount to a re-utilisation of the databases which were searched through.[181]

With its recent decision *CV-Online v Melons*, the CJEU seems to pave the way for a possibly more flexible interpretation of the sui generis right's scope of protection.[182] Concerning again a meta search engine, the Court narrowed the notion of 'extraction' or 're-utilisation' of substantial parts to acts which adversely affect the database maker's investment in the obtaining, verification or presentation of a database's content, meaning that the relevant acts 'constitute a risk to the possibility of redeeming that investment through the normal operation of the database'.[183] With its argumentation, the CJEU introduces a flexible balancing of interests test based on the sui generis

---

175 Leistner, M., Antoine, L. and Sagstetter, T., *Big Data*, p. 439.

176 See further Bently, L., Derclaye, E. and others, *Study in support of the evaluation of Directive 96/9/EC on the legal protection of databases*, pp. 30 et seq.; see also Derclaye, E. and Husovec, M., *Sui Generis Database Protection 2.0: Judicial and Legislative Reforms,* pp. 7 et seq.

177 Leistner, M., 'Big Data and the EU Database Directive 96/9/EC: Current Law and Potential for Reform', p. 30.

178 See further in Bently, L., Derclaye, E. and others, *Study in support of the evaluation of Directive 96/9/EC on the legal protection of databases*, pp. 7 et seq, 30 et seq.

179 Leistner, M., 'Big Data and the EU Database Directive 96/9/EC: Current Law and Potential for Reform', p. 30; Drexl, J., *Data Access and Control in the Era of Connected Devices,* p. 76.

180 CJEU, judgment of 9 October 2008, *Directmedia Publishing v Albert-Ludwigs-Universität*, C-304/07, EU:C:2008:552, paragraphs 29 et seq.

181 CJEU, judgment of 19 December 2013, *Innoweb v Wegener*, C-202/12, EU:C:2013:850, paragraphs 37 et seq.

182 CJEU, judgment of 3 June 2021, *CV-Online Latvia v Melons*, C-762/19, EU:C:2021:434.

183 CJEU, judgment of 3 June 2021, *CV-Online Latvia v Melons*, C-762/19, EU:C:2021:434, paragraph 47.

right's specific subject-matter consisting in the database maker's market opportunity to redeem the quantitatively or qualitatively substantial investment in the obtaining, verification or presentation of a database's contents. Compared to the *Innoweb* judgment, this decision constitutes a significant chance and may even be interpreted as shifting towards an '*unfair competition law based-approach*'.[184] It remains to be seen if the CJEU follows this flexible approach further.

Another challenge for defining the scope of the database maker's exclusive rights is the distinction of the extraction and re-utilisation of *substantial* parts from *insubstantial* parts which can only be prevented in case of a repeated and systematic use conflicting with the normal exploitation and unreasonably prejudicing the database maker's interest (see Article 7 (5) Database Directive). Initially, this differentiation was meant to limit the sui generis rights' broad scope in the interest of freedom of competition since it has been introduced as a compromise instead of a provision on compulsory licences.[185] Whether a part is a substantial part has to be assessed quantitively or qualitatively in relation to the investment in the creation of the database.[186] In quantitative terms, the substantiality relates to the volume of the used data in relation to the volume of the contents of the whole database, in qualitative terms to the scale of the investment in the obtaining, verification or presentation of the used part. If a database consists of several separate modules which fulfil the criteria for a database, the substantiality of a part is to be assessed in relation to the respective module.[187]

As a result of the *CV-Online v Melons* judgment, a flexible, unfair competition oriented (misappropriation) interpretation could be applied also to the notion of 'substantial part'. Consequently, the extraction or re-use of a substantial part would have to constitute a risk to the possibility of redeeming the investment through the normal operation of the database. Even though the recent development in European case law has paved the way to a flexible interpretation of the sui generis right's scope, this does not seem sufficient for reducing the potential access and use problems in the context of data-driven business models.

For access to individual-level use data (first case group), the current limitation of the sui generis right's scope will often suffice if the respective data amount to only an insubstantial part in relation to the whole database consisting of a very large number of individual-level datasets. For horizontal data sharing, however, its scope might constitute a significant obstacle as competitors need complete, aggregated datasets – in the best case of different sources.[188] While the access of competitors to aggregated datasets for complementary products or services (second case group) might be solved adequately by applying the flexible balancing of interests as introduced with the *CV-Online v Melons* judgment, in the third case group, access to large aggregated datasets (e.g. training data) of big data conglomerates for developing unrelated products or service could still be denied by invoking a potential sui generis right of the database maker. Although general competition law provides a complementary tool at least in regard to the second case group, due to

---

[184] See for more details of the decision Derclaye, E. and Husovec, M., *Sui Generis Database Protection 2.0: Judicial and Legislative Reforms,* pp. 4 et seq.

[185] Bently, L., Derclaye, E. and others, *Study in support of the evaluation of Directive 96/9/EC on the legal protection of databases*, p. 37.

[186] See CJEU, judgment of 9 November 2004, *British Horseracing Board v Hill*, C-203/02, EU:C:2004:695, paragraphs 69 et seq.

[187] See CJEU, judgment of 5 March 2009, *Apis v Lakorda*, C-545/07, EU:C:2009:132, paragraphs 62 et seq.

[188] Leistner, M., 'Big Data and the EU Database Directive 96/9/EC: Current Law and Potential for Reform', p. 31; also, Leistner, M. as reported in Bently, L., Derclaye, E. and others, *Study in support of the evaluation of Directive 96/9/EC on the legal protection of databases*, p. 57.

its character as mere ex-post and case-by-case instrument, it often would come too late (see further below 3.3.1.a.vi). While access to data in the first and second case group might be solved using the existing tools when conflicting with the sui generis right, at least in regard to the third case group, the sui generis right's scope leads to considerable hold-up and leveraging potential. However, currently, the definition of the sui generis right's scope is characterised by significant legal uncertainty, in particular as it still remains to be seen how the CJEU will develop the newly established unfair competition-oriented interpretation further.[189]

iii. Exceptions and limitations

Article 8 (1) Database Directive defines mandatory minimum rights of the lawful user of a database which cannot be overridden by contract (see Article 15 of the Directive). Presently, only the buyer or licensee of a database are considered lawful users. The mandatory minimum rights set forth in Article 8 (1) are, however, – currently – limited to *insubstantial* parts of the database. As the concept of mandatory minimum rights (which is also contained in Articles 5 and 6 of the Computer Programs Directive) is designed to 'travel' with the qualification as a legitimate user of a database,[190] Article 8 Database Directive would generally qualify as a potential 'anchor' to guarantee legitimate owners of a data capturing product or legitimate users of a data capturing service the access to individual-level use data (first case group).[191] The definition of the lawful user developed under the Computer Programs Directive might potentially serve as model in this regard (see further below).

Article 9 Database Directive sets out general exceptions to the sui generis right for private purposes, teaching or scientific research, public security, and administrative or judicial procedure which are, however, limited to the lawful user. Yet, limiting these exceptions to the lawful user is systematically not compatible with general copyright law: Exceptions define under which conditions the use of a protected subject matter is legitimate and do, therefore, not contain an 'additional legitimacy test' as introduced by Article 9 Database Directive with its limitation to the lawful user.[192] The wording of Article 9 Database Directive, furthermore, implies that solely substantial parts of a database (but not the complete database) can be extracted or re-used. Such delineation, however, does not contribute to solving access problems as competitors or new market entrants need access to complete datasets.

Consequently, the exceptions to the sui generis right are designed very narrowly – in particular when comparing them to the already existing broader copyright exceptions.[193] Furthermore, the exceptions to the sui generis right are not aligned with the general catalogue of exceptions and limitations for copyrighted works defined in the InfoSoc Directive. However, such alignment and even more a dynamic linking would be strongly desirable. At least the important exceptions for text

---

189 See also Calatrava Moreno and others, *Study to Support an Impact Assessment for the Review of the Database Directive*', p. 8.

190 See for the Computer Programs Directive CJEU, judgment of 3 July 2012, *Used Soft v Oracle*, C-128/11, EU:C:2012:407, paragraphs 80 et seq.

191 Leistner, M., 'Big Data and the EU Database Directive 96/9/EC: Current Law and Potential for Reform', pp. 41 et seq.

192 Leistner, M., 'Big Data and the EU Database Directive 96/9/EC: Current Law and Potential for Reform', p. 48.

193 See already Kur, A., and others, 'First Evaluation of Directive 96/9/EC on the Legal Protection of Databases – Comment by the Max Planck Institute for Intellectual Property, Competition and Tax Law, Munich', *International Review of Intellectual Property and Competition Law,* 2006, pp. 551 et seq.

and data mining, which were adopted with Articles 3 and 4 DSM Directive[194] (see further below 3.2.3), are explicitly applicable to the sui generis right and copyrightable databases.

Due to the specific character of the sui generis right, also traditional copyright exceptions regulated in the Member States do not apply.[195] This becomes particularly problematic for databases of public bodies: While in certain Member States copyright protection is excluded for official works by public bodies, the sui generis right would in principle apply to databases of public bodies.[196] Protecting databases of public bodies under the sui generis right would, however, create considerable tension not only with the Open Data Directive and the Data Governance Act but also with the more general objective of enhancing G2B data sharing. Both the Open Data Directive (in its Article 1 (6)) and the planned Data Governance Act (in its Article 5 (7)) contain at least provisions according to which the sui generis right 'shall not be exercised by public sector bodies in order to prevent the re-use of documents or to restrict re-use'. However, it should all the more be clarified that public body databases do not qualify for sui generis protection.

iv. Ownership and the database maker

Article 7 (1) Database Directive refers to the database maker as relevant owner of the sui generis right. Recital 41 of the Directive specifies in that regard that 'the person who takes the initiative and the risk of investing' is to be qualified as the database maker while subcontractors are excluded from this definition. Many scenarios of data-driven innovation and particularly data sharing networks or industrial data platforms are, however, characterised by cooperative structures involving a multitude of players. In these cases, each participant bears at least the risk for its own investment and can, therefore, qualify as database maker leading to joint ownership of the database. Intensified by the fact that in practice the participants of cooperative networks are often not conscious about such results, in the context of access rights, joint ownership leads to legal uncertainty and high information and transaction costs, e.g. for identifying all rightholders and carrying out negotiations. However, for the time being, it would not be reasonable to allocate the sui generis right differently as potential data sharing scenarios are very diverse and data markets are still developing dynamically. Consequently, it should be left open to the participants of data sharing networks to agree on a particular allocation of the sui generis right by means of contract. Currently, it remains legally uncertain how to design respective contract terms in practice as so far sound standards or established guidelines other than the quite abstract best practices provided by the European Commission (see above 3.1.8.b) do not exist. Notably, the Trade Secrets Directive imposes a similar ownership problem which we will address further below (3.2.4).

v. Interface with unfair competition law and general overlap problems

According to its Article 13, the Database Directive shall be without prejudice to other provisions or any other rights or obligations the data are subject to – including most prominently unfair

---

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

[195] Kur, A., and others, 'First Evaluation of Directive 96/9/EC on the Legal Protection of Databases – Comment by the Max Planck Institute for Intellectual Property, Competition and Tax Law, Munich', *International Review of Intellectual Property and Competition Law,* 2006, p. 557.

[196] See for instance German Federal Supreme Court (BGH), judgment of 25 March 2010, *Autobahnmaut*, I ZR 47/08.

competition law. The provision is interpreted as allowing for the protection of data compilations under national unfair competition law even if the requirements of the sui generis right are not fulfilled. However, the details of protection under national unfair competition law vary widely,[197] contradicting thereby the Directive's objective to harmonise the protection of databases in the European Union. In addition, applying unfair competition law would undermine the already comprehensively balanced interests expressed in the Directive by assigning databases which do not fulfil the conditions for protection to the public domain.[198]

Further overlap problems may also arise in regard to the individual rights set forth in the GDPR (in particular portability, Article 20, and access, Article 15 GDPR) as far as personal data is concerned. The GDPR provides certain balancing of interest clauses which restrict the data subject's rights if they affect the rights and freedoms of others, see e.g. Article 15 (4) and Article 20 (4) GDPR. Contrary to the GDPR's explicit provisions, the Digital Content Directive with its B2C portability right of non-personal data after contract termination[199] and also the access and portability rights foreseen in the proposal for a Digital Markets Act do not touch upon possible conflicting rights such as the sui generis right.

vi. Term of protection

According to Article 10 Database Directive, databases are protected under the sui generis right for 15 years. However, looking at the typical exploitation periods of electronic databases, this term of protection is far too long – all the more in the context of a continuously growing data-driven economy.[200] Correspondingly, already in the evaluation of the Database Directive 2018, the duration of 15 years has been criticised intensively.[201] The supporting scientific study, therefore, has suggested to shorten the term of protection to five years.[202] Due to the renewal of protection for any substantial change or update of the database (for again 15 years), continuously updated databases could thus qualify for 'perpetual protection'. However, this can be avoided under the current lex lata, for instance by defining the term 'substantial part' specifically for such updated databases.[203]

vii. Summary

As a result of its current scope, the sui generis rights might play a significant role in a European data economy. This is because many datasets processed in typical big data scenarios, including certain

---

[197] For an overview see Bently, L., Derclaye, E. and others, *Study in support of the evaluation of Directive 96/9/EC on the legal protection of databases*, pp. 87 et seq.; see for instance German Federal Supreme Court (BGH), judgment of 6 Mai 1999, *Tele-Info-CD*, I ZR 199 / 96.

[198] Leistner, M., 'Big Data and the EU Database Directive 96/9/EC: Current Law and Potential for Reform', pp. 54 et seq.

[199] See Article 16 (4).

[200] Leistner, M., 'Big Data and the EU Database Directive 96/9/EC: Current Law and Potential for Reform', p. 50.

[201] See for an overview over results of the public consultation Commission Staff Working Document, *Evaluation of Directive 96/9/EC on the legal protection of databases*, SWD(2018) 146 final, 2018, p. 58.

[202] Bently, L., Derclaye, E. and others, *Study in support of the evaluation of Directive 96/9/EC on the legal protection of databases*, p. vii. The authors referred to the similar term of protection of a comparable database right in South Korea, see pp. 80, 132 et seq.

[203] See in this regard already Leistner, M., 'Legal Protection for the Database Maker – Initial Experience from a German Point of View', *International Review of Intellectual Property and Competition Law,* 2002, pp. 458 et seq.

types of machine-data, could qualify for protection. Even if in practice the sui generis right might only have very limited impact (as mere ex-post instrument[204]), it could thus be invoked by the rightholder against access and portability rights. The sui generis right could, therefore, intensify the problem of de facto control over data leading to significant access problems and even hold-up potential. In particular, there is significant legal uncertainty in regard to core elements of sui generis protection, such as the distinction between collection and creation of data, the notion of 'substantial part' and other.

3.2.3. General Copyright Law: exceptions and limitations for text and data mining

As data itself is not protected under Copyright (or any other IP right either) and structuring of data is covered by the sector-specific provisions for database protection, general copyright provisions do only play a marginal role for the question of data sharing and open data. However, the importance of the exceptions for text and data mining should be stressed as they constitute the legal basis for creating databases or data compilations where the analysed materials are protected under copyrights. These exceptions implemented in Article 3 (for scientific research) and Article 4 (as general exception) of the DSM Directive set out a rather strict standard, inter alia data mining for scientific research may only be carried out for non-commercial purposes. Therefore, these exceptions could potentially be too narrow for facilitating text and data mining as one important tool for the creation and aggregation of data and datasets.

Comparing the scope of the copyright exceptions for text and data mining with other jurisdictions, the EU lags behind:[205] Japan for instance has introduced a flexible copyright exception for 'non-enjoyment' purposes which expressly covers any exploitation for text and data mining activities, even for commercial purposes.[206] US copyright with its fair use clause provides in general a higher level of flexibility and qualifies text and data mining as potential fair use.[207] Notably, China has not introduced an explicit exception for text and data mining to the closed list of exceptions in course of the recent copyright reform. However, as Chinese courts generally interpret the (modified) three-step test, which was implemented in 2013[208] as enabling instrument, sufficient flexibility to deal with text and data mining cases seems to be given in practice. As this comparative perspective shows, the European copyright exceptions for text and data mining are insufficiently narrow for dealing with text and data mining as core activity in a data-driven economy.

---

[204] See Bently, L., Derclaye, E. and others, *Study in support of the evaluation of Directive 96/9/EC on the legal protection of databases*, pp. 95 et seq.

[205] See also Geiger, C., Frosio, G. and Bulayenko, O., 'Text and Data Mining in the Proposed Copyright Reform: Making the EU Ready for an Age of Big Data?', *International Review of Intellectual Property and Competition Law,* 2018, pp. 814 et seq.

[206] Article 30-4 Japanese Copyright Act. See further Ueno, T., 'The Flexible Copyright Exception for 'Non-Enjoyment' Purposes – Recent Amendment in Japan and Its Implication', *Gewerblicher Rechtsschutz und Urheberrecht Internationaler Teil*, 2021, p. 145 et seq.

[207] 17 U.S. Code US Copyright Act § 107. See for instance United States Court of Appeals, 2nd. Cir., judgment of 16 October 2015, *Authors Guild v Google*, 804 F.3d 202.

[208] Lee, J. and Li, Y. 'The Pathway Towards Digital Superpower: Copyright Reform in China', *Gewerblicher Rechtsschutz und Urheberrecht Internationaler Teil,* 2021, p. 867.

3.2.4. Trade Secrets Directive

In the context of the Data Act, the Commission has also referred to a 'clarification of certain key provisions of the Trade Secrets Directive'.[209] The protection of trade secrets does not amount to an absolute 'intellectual property right'. However, the Trade Secrets Directive[210] provides the rightholder with effective remedies against the unlawful acquisition, use, and disclosure of secret information. As a result of the broad definition of the term 'trade secret' (see Article 2 (1) Trade Secrets Directive and corresponding Recital 14) all core elements of a data-driven economy, such as diverse forms of datasets (including meta-data, excluded however a single datum), algorithms, program code or interface information can generally qualify for protection.[211] The same holds true for co-generated data and individual use data because the combination and aggregation of large datasets gives rise to the necessary commercial value of such data.[212] As a result, trade secret protection has become key instrument for both the protection of data and the trading of data.

The relevant information has to be kept secret (not generally known in the relevant circle) and subject to reasonable steps for maintaining its secrecy. The notion of 'reasonable steps for maintaining secrecy', which is based on Article 39 TRIPS, should be interpreted broadly as otherwise tension with the general objective of trade secret protection to save transaction costs for protection measures would arise. Moreover, a rigid interpretation could prevent trade secret holders from sharing data in cooperative networks or data pools.[213]

The definition of the 'trade secret holder' in Article 2 (2) of the Directive referring to 'any natural or legal person lawfully controlling a trade secret' remains quite vague.[214] In cooperative data sharing or data pooling networks, this definition would – comparable to the database sui generis right – lead to multiple joint ownership. By means of contract law, the participating entities may obviously agree on a different allocation. However, as the Trade Secrets Directive is silent about contract law and licensing, there is still significant legal uncertainty. Furthermore, as already observed in the context of the sui generis right, lacking standards for contract law might lead to transaction and information costs. These inefficiencies could be remedied by introducing non-mandatory contract clauses, developing standard terms, and/or best practices.

Currently, there are certain inconsistencies between the Trade Secrets Directive and the above-mentioned mandatory exception for the decomplication of computer programs for interoperability purposes regulated in Article 6 Computer Programs Directive. Reverse engineering and, therefore, also the decomplication of a computer program are considered as 'lawful means of acquiring information, except when otherwise contractually agreed' under the Trade Secrets Directive (Recital

---

209 European Commission, *Intellectual Property Action Plan*, COM(2020) 760 final, pp. 13 et seq.; European Commission, *Inception Impact Assessment*, Ref. Ares(2021)352715, 28 May 2021, p. 1.

210 Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (hereinafter 'Trade Secrets Directive').

211 Drexl, J., *Data Access and Control in the Era of Connected Devices*, pp. 92 et seq.

212 See already Commission Staff Working Document, *on the free flow of data and emerging issues of the European data economy, Accompanying the document Communication Building a European data economy*, SWD(2017) 2 final, p. 20: 'It is doubtful that individual data generated by interconnected machines and devices could be regarded as "trade secret" in the sense of this Directive, mostly because of its lack of commercial value as individual data; however, combination of data (datasets) can be trade secrets under this Directive if all the criteria are met.' Aplin, T., 'Trading Data in the Digital Economy: Trade Secrets Perspective', pp. 65 et seq.

213 Leistner, M., 'The existing European IP rights system and the data economy', p. 233.

214 Aplin, T., 'Trading Data in the Digital Economy: Trade Secrets Perspective', p. 69.

16 and 17). While Article 6 Computer Programs Directive cannot be overridden by contract (see Article 8 Computer Programs Directive), under the Trade Secrets Directive reverse engineering can be prohibited by contract.

In sum, Trade Secret protection, on the one hand, intensifies de facto control over data and even over information needed for interoperability such as for instance interface specifications. On the other hand, it has to be assessed very carefully under which conditions existing and future access and portability rights should extend to secret information. From a competition law perspective, access to information can be granted under the strict requirements of Article 102 TFEU even if trade secrets are concerned.[215]

3.3. Need for action

3.3.1. Database Directive

a. Proposed amendments of the Database Directive

As shown above, the database sui generis right has significant relevance for both protection of databases and access to data in the European data economy. The current acquis intensifies factual control over data and thus aggravates the existing access problems or can even result in hold-up potential in certain situations. In particular, due to the legal uncertainty in regard to several central concepts – concerning even the very conditions of protection – the sui generis right currently causes considerable information and transaction costs.

i. Specification of conditions of protection for machine-generated data

The database sui generis right's conditions of protection should be specified for machine-generated data since the established distinction between 'collection' and 'creation' of data is currently uncertain and, moreover, not entirely suitable for defining the scope in this context. One potential option would, therefore, be to combine the clarification of the open-ended umbrella definition of relevant investments with a catalogue of certain exemplary non-conclusive (positive) case groups, in which sui generis protection might be needed in order to set incentives (possibly inferred high-quality training data), and possibly also (negative) case groups in which this is evidentially not the case (possibly certain types of (volunteered/observed) machine-generated data).

ii. Reform of exceptions and limitations

The exceptions and limitations for the sui generis right are in imminent need of reform.[216] This is particularly the case as the sui generis right's limitation to the use of substantial parts and the

[215] See Court of First Instance, order of 22 December 2004, *Microsoft v Commission,* T-201/04 R, EU:T:2004:372 and judgment of 17 September 2007, *Microsoft v Commission*, T-201/04, EU:T:2007:289.

[216] Derclaye, E. and Husovec, M., *Sui Generis Database Protection 2.0: Judicial and Legislative Reforms,* pp. 10 et seq.; Bently, L., Derclaye, E. and others, *Study in support of the evaluation of Directive 96/9/EC on the legal protection of databases*, pp. 15 et seq.

existing limitations do not suffice for facilitating the re-use of data in the identified case groups of justifiable access to data.

First, Article 8 Database Directive, which defines the lawful user's mandatory minimum rights, should be extended to not only insubstantial parts of a database but also to substantial parts and even the entire database.[217] In addition, the concept of 'lawful user' should be revised and not only applied to the buyer or licensee of a database but to legitimate owners of a data capturing product or legitimate users of a data capturing service. In a similar vein, the CJEU re-defined the interpretation of the lawful user under the Computer Programs Directive in its UsedSoft judgment: In context of the exhaustion of the distribution right, the Court decided that not only the first acquirer of a computer program but any subsequent acquirer of it can rely on the exhaustion of the distribution right and therefore be regarded as lawful acquirer.[218] On this basis, Article 8 of the Database Directive could serve as important tool for facilitating the access, re-use and portability of individual-level use data (first case group) by complementing specific access rights in this particular field.

Moreover, first, it should be assessed further whether the Database Directive itself can contribute to a more coherent approach in regard to already existing (e.g. Article 20 GDPR) or future (possibly arising from the Digital Markets Act) access and portability rights, for instance by introducing an explicit exception for these cases with the result that a database maker would not be able to invoke the sui generis right against the exercise of such an access or portability right.[219]

Second, the exceptions set forth in Article 9 Database Directive should not be limited to the extraction and re-use of the lawful user but should furthermore be extended to use acts regarding the complete databases. Furthermore, the strict limitation of the exceptions to non-commercial uses has to be put under scrutiny.

Third, the exceptions defined for copyrighted database works should also apply to databases protected under the sui generis right. The exceptions defined in the Database Directive should at least be aligned and dynamically linked with the exceptions and limitations set forth in the InfoSoc Directive.[220] Additional exceptions for safeguarding reverse engineering and interoperability, both for databases protected through the sui generis right and through copyright, should be considered in order to guarantee the relevant infrastructure for data sharing, access, and portability.[221] The exception for the decomplication of computer programs for interoperability purposes (Article 6 Computer Programs Directive) can serve as a first model in this regard, even though the requirements set forth in the Computer Programs Directive are rather high.

Fourth, in order to enhance G2B data sharing and to avoid inconsistency with the Open Data Directive, an exception for databases of public bodies is indispensable.[222]

---

[217] Cf. Bently, L., Derclaye, E. and others, *Study in support of the evaluation of Directive 96/9/EC on the legal protection of databases*, pp. 74 et seq.

[218] CJEU, judgment of 3 July 2012, *Used Soft v Oracle*, C-128/11, EU:C:2012:407, paragraphs 73 et seq.

[219] Leistner, M., Antoine, L. and Sagstetter, T., *Big Data,* pp. 447 et seq.

[220] Bently, L., Derclaye, E. and others, *Study in support of the evaluation of Directive 96/9/EC on the legal protection of databases*, pp. 15 et seq., 58 et seq.

[221] Leistner, M., 'Big Data and the EU Database Directive 96/9/EC: Current Law and Potential for Reform', pp. 52 et seq.

[222] Bently, L., Derclaye, E. and others, *Study in support of the evaluation of Directive 96/9/EC on the legal protection of databases*, p. 121. See also Commission Staff Working Document, *Evaluation of Directive 96/9/EC on the legal protection of databases*, SWD(2018) 146 final, 2018, pp. 40 et seq., p. 46 in regard to the former PSI Directive.

iii. Term of protection

The protection term of fifteen years does not correspond with the needs of a data-driven economy and may intensify de facto control.[223] The term of protection should, therefore, be reduced to a maximum of three years.[224] A systematic comparison with the protection of unregistered community designs[225] can serve as argument for the particular period of three years. Both, unregistered community designs and the sui generis right are expression of a two-fold protection for the respective subject matter covering a specific purpose (registered versus unregistered design and copyright protection versus sui generis right for databases). Comparable to the sui generis right's function to protect a substantial investment in a database, the protection of unregistered designs solely prevents the imitation of the protected design.[226]

iv. Ownership and (non-mandatory) model contract terms

The definition of 'database maker' leads to joint ownership in cooperative networks for data sharing or pooling.[227] In this regard, legislative action is not needed but rather best practices, models and/or guidelines for non-mandatory contract law should be developed for reducing legal uncertainty, transaction costs and potential information asymmetry. This aspect holds generally true for the licensing of databases under the sui generis right and non-mandatory model contract terms or best practices should, therefore, not be limited to the ownership issue but address generally the conditions for input, extraction, and use of data in multipolar big data settings.[228]

v. Interface with unfair competition law and further overlaps

Moreover, the interface with Member States' unfair competition law protection instruments should be clarified by introducing a provision which ensures the pre-emption of national unfair competition law for cases falling within the scope of the Database Directive.[229] In order to guarantee a uniform standard for the protection of databases, a respective provision has to clarify that national unfair competition law protection against copying of databases only applies where the use of a database is characterised by additional circumstances specifically regulated by unfair competition law and beyond the mere objective of competitors' protection against misappropriation; practically, this would limit the remaining realm for the application of unfair competition law to cases of consumer confusion. If the scope of the sui generis right is limited in a way, for instance not including certain types of machine-generated data, this would require the clarification that such compilations shall not be protected under (national) unfair competition law either.[230]

---

[223] Bently, L., Derclaye, E. and others, *Study in support of the evaluation of Directive 96/9/EC on the legal protection of databases*, p. 80.

[224] Cf. Leistner, M., Antoine, L. and Sagstetter, T., *Big Data,* p. 418 proposing a range from three to five years.

[225] See Article 11 Council Regulation (EC) No 6/2002 of 12 December 2001 on Community designs.

[226] Article 19 (2) Council Regulation (EC) No 6/2002 of 12 December 2001 on Community designs.

[227] Bently, L., Derclaye, E. and others, *Study in support of the evaluation of Directive 96/9/EC on the legal protection of databases*, pp. 31 et seq.

[228] Leistner, M., 'Big Data and the EU Database Directive 96/9/EC: Current Law and Potential for Reform', p. 39.

[229] Bently, L., Derclaye, E. and others, *Study in support of the evaluation of Directive 96/9/EC on the legal protection of databases*, p. 87 et seq; Leistner, M., 'Big Data and the EU Database Directive 96/9/EC: Current Law and Potential for Reform', p. 54; Derclaye, E. and Husovec, M., *Sui Generis Database Protection 2.0: Judicial and Legislative Reforms,* pp. 11 et seq.

[230] Derclaye, E. and Husovec, M., *Sui Generis Database Protection 2.0: Judicial and Legislative Reforms,* pp. 12 et seq.

vi. Compulsory licences

As the analysis has shown, certain case groups in the data-driven economy require access to complete datasets, in particular by competitors to establish workable competition in aftermarkets or complementary markets (second case group) or by third parties for developing unrelated products or services (third case group).

Where access to such datasets is granted as a result of particular regulation (see above 3.1), the database sui generis right might, however, be invoked by the rightholder. Currently, the database sui generis right's limitation to substantial parts merely facilitates access to individual-level use data (first case group) being an insubstantial part of the content of a database but does not address the second and third case group adequately (see already above 3.2.2.b.ii). Therefore, introducing compulsory licensing for those case groups might be an effective means for guaranteeing the right to re-use the relevant datasets.[231] In general, there are three possible ways, first, by relying on competition law, second, by introducing a specific provision in the Database Directive itself (IP internal approach), and, third, by introducing area-specific access legislation which would then have to comprise compulsory licences concerning possibly affected intellectual property rights. As general competition law with its Article 102 TFEU has the specific objective to avoid exclusionary conduct in order to guarantee effective competition and to allow follow-on innovation, it does not apply to all of the defined case groups of justifiable data access (see above 3.1.5). In addition, competition law is a mere ex-post instrument sanctioning a particular conduct which often might 'come too late' because the high thresholds for intervention have to be established in long lasting proceedings.

Introducing a compulsory licence regime to the Database Directive could be a way to solve the two problematic constellations of sole source databases and public body databases. The Commission's initial proposal for a Database Directive included provisions on compulsory licences in its Article 8.[232] The provision foresaw a compulsory licence under 'fair and non-discriminatory' terms for publicly available sole source databases and for publicly available databases compiled by public bodies – it was, hence, designed to cover solely databases which were already made available to the public.[233] The limited scope was proposed in order to protect sensitive information, it would have, however, been too narrow to cover the relevant case groups comprehensively.[234] While a provision based on this original proposal facilitates the re-use of the huge number of databases which are (directly or indirectly) available to the public, it does not provide a solution for sole source or public body databases as such. As regards data compilations by public bodies, it has therefore been proposed to introduce an explicit exception in order to exclude such databases from protection – comparable to the exclusion of official works by public bodies from copyright protection (see above 3.2.2.b.iii). Since the CJEU's approach to exclude sole source databases from sui generis protection by distinguishing between the 'creation' and 'collection' of data (see above 3.2.2.b.i) is characterised by legal uncertainty, sole source situations should be prevented pro-actively by providing for

---

[231] Bently, L., Derclaye, E. and others, *Study in support of the evaluation of Directive 96/9/EC on the legal protection of databases*, pp. 34 et seq.; Leistner, M., Antoine, L. and Sagstetter, T., *Big Data,* pp. 451 et seq. Derclaye, E. and Husovec, M., *Sui Generis Database Protection 2.0: Judicial and Legislative Reforms,* pp. 9 et seq.

[232] See Commission, *Proposal for a Council Directive on the legal protection of databases*, OJ C 156, 23.6.1992, p. 4.

[233] Also Ginsburg proposed in her seminal paper to limit a compulsory licence regime to 'publicly disclosed data bases', see Ginsburg, J., 'Creation and Commercial Value: Copyright Protection of Works of Information', *Columbia Law Review*, Vol. 90, 1990, p. 1925.

[234] Bently, L., Derclaye, E. and others, *Study in support of the evaluation of Directive 96/9/EC on the legal protection of databases*, p. 41.

compulsory licensing in this regard.[235] The definition of 'sole source database' should thereby follow the indispensability criterion as developed in the CJEU's *Bronner* decision.[236] This would require firstly, that creating a comparable database would not be economically viable for a competitor whose size and resources are comparable to those of the original database maker.[237] Secondly, accessing the relevant datasets would have to be indispensable for access to a downstream market in relation to the (hypothetical) upstream licensing market for the data.[238] Such licence should be granted only for payment of remuneration based on fair, reasonable and non-discriminatory terms. In order to give the concept of FRAND further substance, a compulsory licence regime could emphasise the parties' possibility to agree on cross (reciprocal) licences as it has been proposed (as condition) for compulsory licences under general competition law.[239] Potentially, an arbitration mechanism could serve as procedural backup for negotiating the FRAND conditions.[240]

b. Possible further policy options

Already the evaluations in 2005 and 2018 named the *complete abolition* of the sui generis right as a possible option in order to avoid potential dysfunctional effects.[241] In the context of enhancing data-driven innovation, fostering data sharing, and facilitating the development of a European data economy, it should be put under scrutiny to what extent the sui generis right is still appropriate to fulfil its incentive rational and whether it might have shifted to a mere obstacle to disseminating data.

As less invasive but still fundamental change the transformation of the sui generis right into a *registered industrial property right* has been discussed.[242] Such right would require registration and the payment of continued fees (which could for instance increase until reaching a maximum protection time which would be to define) and would generally be granted initially only for a short protection period. Implementing a registered right could however all the more lead to 'strategic' registration which might result in even higher blocking potential. Moreover, a new, formal and in practice (potentially) very complicated layer would be added to the sui generis right already characterised by immense legal uncertainty.[243]

---

235 Leistner, M., 'Big Data and the EU Database Directive 96/9/EC: Current Law and Potential for Reform', pp. 44 et seq.; Leistner, M., 'The existing European IP rights system and the data economy', pp. 243 et seq.

236 Leistner, M., 'The existing European IP rights system and the data economy', pp. 243 et seq.

237 Cf. CJEU, judgment of 26 November 1998, *Oscar Bronner v Mediaprint*, C-7/97, EU:C:1998:569, paragraphs 46 et seq.; Leistner, M., 'The existing European IP rights system and the data economy', pp. 244 et seq.

238 Leistner, M., 'The existing European IP rights system and the data economy', p. 245.

239 See Schweitzer, H., 'Datenzugang in der Datenökonomie: Eckpfeiler einer neuen Informationsordnung', *Gewerblicher Rechtsschutz und Urheberrecht*, 2019, p. 579.

240 An obligation for granting cross licences does not seem to have regulated in the Database Directive but can be left open to be assessed by the competent authority or the courts.

241 Bently, L., Derclaye, E. and others, *Study in support of the evaluation of Directive 96/9/EC on the legal protection of databases*, pp. 122 et seq.

242 Bently, L., Derclaye, E. and others, *Study in support of the evaluation of Directive 96/9/EC on the legal protection of databases*, pp. 65 et seq.; Leistner, M., 'Big Data and the EU Database Directive 96/9/EC: Current Law and Potential for Reform', pp. 38 et seq.; Leistner, M., Antoine, L. and Sagstetter, T., *Big Data,* pp. 418 et seq.

243 Leistner, M., 'Big Data and the EU Database Directive 96/9/EC: Current Law and Potential for Reform', p. 38.

3.3.2. Interface with trade secrets protection

An imminent need for action arises at the interface of data access and use rights with trade secrets protection. Protection of trade secrets is justified as incomplete information is a substantial condition for functioning and competitive markets, where such trade secrets concern market information or other information on parameters of competition.[244] Beyond that, trade secrets protection serves the purpose of reducing transaction cost (for the implementation of cost-intensive factual protection measures) and fostering contractual sharing of information (through providing legal certainty and thus solving 'prisoner dilemmas').

For information underlying trade secret protection, therefore it has to be carefully assessed under which conditions access to the (secret) information should be granted and whether and to which extent an 'access regime' should also cover the subsequent *use* of the respective information. The Trade Secrets Directive does not only protect against the unlawful *acquisition* (Article 4 (2)), but also against unlawful *use* or *disclosure* (Article 4 (3)) of a trade secret. The use or disclosure of a trade secret is deemed unlawful when the information was already acquired unlawfully or even when the trade secret was disclosed or used in breach of a contractual or any other duty. According to Articles 4 (4) and 4 (5) Trade Secrets Directive, the protection extends further to certain acts of third parties if they knew or ought to have known that the trade secret was acquired, disclosed or used unlawfully. Remarkably, this even covers the production or offering of infringing goods, i.e. goods which significantly benefit in their design, characteristics, functioning, production process or marketing from unlawfully required, used or disclosed trade secrets (see Articles 4 (5), 2 (4) Trade Secrets Directive).

The Trade Secrets Directive itself sets out that the acquisition, use or disclosure shall be considered lawful to the extent that such acquisition, use or disclosure is *required or allowed* by Union or national law, see Article 3 (2) Trade Secrets Directive. Furthermore, it provides an exception for the acquisition, use or disclosure of a trade secret for the purpose of protecting a *legitimate interest* recognised by Union or national law (5 (d) Trade Secrets Directive). Along these lines, access rights foreseen in the acquis could thus generally be qualified as a relevant legitimate interest or obligation recognised/set out by Union law. Due to the sensitive character of trade secrets, it seems preferable to apply stricter standards than for access to IP protected subject matters and to develop case groups in which the interest of access prevails compared to the interest to protect secret information. At the end of the day, the most cautious option would be to rely on a competition law approach, i.e. granting access to trade secrets only under the strict conditions of Article 102 TFEU.[245]

However, in light of the objective for protecting trade secrets as 'competitive advantage' two case groups should be distinguished:[246] Market-related *business information* pertaining to competition parameters and the competitive process as such (data on clients, profiles, pricing, business strategies etc.) should be made available solely under the prerequisites of a compulsory licence under Article 102 TFEU. In regard to *technical or creative know-how* related to a creation or innovation which potentially qualifies for IP protection the same standard as for allowing access and use of IP-protected subject matters should be applied.

---

[244] See e.g. Recitals 1 and 2 of the Trade Secrets Directive.

[245] See in this regard Court of First Instance, order of 22 December 2004, *Microsoft v Commission,* T-201/04 R, EU:T:2004:372 and judgment of 17 September 2007, *Microsoft v Commission*, T-201/04, EU:T:2007:289.

[246] See already Leistner, M., Antoine, L. and Sagstetter, T., *Big Data,* pp. 432 et seq.; Leistner, M., Towards an Access Paradigm in Innovation Law?, *Gewerblicher Rechtsschutz und Urheberrecht Internationaler Teil*, 2021, pp. 929 et seq.

3.3.3. Personal vs non-personal data

Due to the importance of the fundamental rights guaranteeing respect for private and family life (Article 7 of the Charta[247]) and protection of personal data (Article 8 of the Charta) the legal framework distinguishes clearly between *personal data* and *non-personal data*. However, there is need to align the rules on sharing of non-personal data and personal data.[248] Even when following an approach of a strict distinction between access to and portability of non-personal data and personal data, i.e. by designing provisions for non-personal data without prejudice to the GDPR, it should at least be considered to define the notion of personal data more specifically.[249] Otherwise, especially for stakeholders, it will not be possible to evaluate with sufficient legal certainty under which regime data flows would fall. This is of particular importance since an anonymisation of personal data has become nearly impossible because the increasing amount of data and the quality of big data analytics often allow to trace data back and re-identify a natural person (i.e. in the case of small businesses and many other situations).[250] To meet this challenge, e.g. the US and Japan, have developed models for anonymising data which consist in both technical and organisational measures in order to reduce the risk of a re-identification of a natural personal as data subject.[251] Based on these approaches, *technical* standards for the anonymisation of data should be developed and supported by respective *organisational obligations* such as a commitment to refrain from re-identifying personal data. As far as these requirements are fulfilled, a *rebuttable presumption* that the respective data is considered as anonymised – thus, non-personal – data could apply in order to provide legal certainty with respect to the non-applicability of the GDPR.[252] Such presumption could be made subject to further restrictions, such as to a limited time of validity or to particular methods of data processing.[253] Notably, the Commission proposes in Article 28 (3) and Article 30 (4) of the Data Act a technically comparable presumption that the requirements of the respective provisions are fulfilled if 'the harmonised standards or parts thereof published by reference in the Official Journal of the European Union' are met. This regulatory technique can serve as a first example, even though standards for the anonymisation of data still would have to be developed.

3.3.4. Portability

Since Article 20 GDPR entered into force, it has been intensively discussed whether a right to portability of non-personal data should be implemented as *general principle*. Due to the (expected) pro-competitive effect arising from reduced lock-in effects and lower switching costs, it has been

---

247 Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012, p. 391–407 (hereinafter 'Charta').

248 Cf. Picht, P. and Richter, H., *The Proposed EU Digital Services Regulation 2020: Data Desiderata*, p. 14.

249 See also Graef, I., Husovec, M. and van den Boom, J., 'Spill-Overs in Data Governance: Uncovering the Uneasy Relationship Between the GDPR's Right to Data Portability and EU Sector-Specific Data Access Regimes', *Journal of European Consumer and Market Law,* 2020, pp. 14 et seq.; Graef, I., Gellert, R. and Husovec, M., 'Towards a Holistic Regulatory Approach for the European Data Economy: Why the Illusive Notion of Non-Personal Data is Counterproductive to Data Innovation', *European Law Review*, 2019, pp. 605 et seq.

250 See for instance, ENISA, *Privacy by design in big data*, pp. 27 et seq.

251 In the US the concept is discussed as 'personally identifiable information', see further US Federal Trade Commission, *Protecting Consumer Privacy in an Era of rapid Change*, Report, 2012, p. 18 et seq. In Japan the new category of 'Anonymously Processed Information' has been introduced to Articles 36 et seq. of the Act on the Protection of Personal Information in 2018 (available at: https://www.ppc.go.jp/files/pdf/APPI_english.pdf).

252 The German Data Ethics Commission has proposed to introduce a respective system, see its *Opinion*, p. 131.

253 German Data Ethics Commission, *Opinion*, p. 131.

argued that a general data portability right might have the potential to incentivise sharing data.[254] The Regulation on the free flow of non-personal data (self-regulatory approach for cloud switching), the Digital Contents Directive (post-contractual B2C obligations) and the planned Digital Markets Act (in relation to gatekeepers)[255] have taken up these considerations and implemented portability rights for particular case groups.

However, with the passage of time – and with first experiences in regard to Article 20 GDPR –, it has turned out that the effectiveness of portability rights depends highly on, first, the users, and second, the practicable, i.e. *technical*, feasibility.[256] Interoperability of data formats, the implementation of import and export mechanisms, accessible APIs etc. are substantial technical barriers for establishing effective data portability. Implementing the necessary tools and mechanisms, requires high costs for the providers which can result in significant barriers for new market entrants.[257] Thus, it has been concluded that firms with an already strong market position and 'data stock' might benefit the most from portability rights.[258] Consequently, the need for introducing portability rights in order to reduce lock-in effects and, vice versa, the positive pro-competitive effects of such right, vary depending on the particular sector and have therefore to be assessed in detail.[259] Against this background, the more tentative, sector-specific approach to introducing portability rights which becomes apparent in the mentioned legal acts, deserves support.

3.3.5. Measures for enhancing interoperability

In light of the existing technical barriers to functioning data sharing and data portability, a framework of technical standards and further measures for enhancing interoperability should be developed. First of all, this applies to the data models and formats in which data are stored, processed and exchanged. However, the used data formats depend on the type and category of data (e.g. structured, semi-structured, unstructured data) and are characterised by different advantages and disadvantages.[260] Not only the format as such (syntax) but also the vocabulary or semantics have to be aligned for effective data exchange.[261] In addition, the storage of data can be organised differently (database management systems) being of particular relevance for real-time data transfer.[262] Data transfer or exchange as such requires accessible and uniform APIs.[263] On a more organisational level, the modes of exporting or transferring data can vary and therefore complicate effective data sharing.[264] In sum – and most importantly –, *common data formats* and *accessible*

[254] See also European Commission, *Building A European Data Economy*, COM(2017) 9 final, 2017, p. 15.

[255] See in detail above 3.1.7. Furthermore, general competition law might apply in cases of abuse of a dominant position, see 3.1.5.

[256] Graef, I., 'The opportunities and limits of data portability for stimulating competition and innovation', *Competition Policy International – Antitrust Chronicle*, 2020, pp. 2 et seq.

[257] See already, European Commission, *Building A European Data Economy*, COM(2017) 9 final, 2017, p. 15.

[258] See above 3.1.1.

[259] Cf. Crémer, J., de Montjoye, Y. and Schweitzer, H., *Competition Policy for the digital era*, pp. 58 et seq., 82 et seq.

[260] Centre on Regulation in Europe (CERRE), *Making Data Portability More Effective for the Digital Economy*, p. 37 et seq.

[261] See with respect to the portability right of the GDPR: Deloitte, *GDPR Data Portability and Core Vocabularies*, Study prepared for the European Commission.

[262] Centre on Regulation in Europe (CERRE), *Making Data Portability More Effective for the Digital Economy*, p. 39 et seq.

[263] Centre on Regulation in Europe (CERRE), *Making Data Portability More Effective for the Digital Economy*, p. 40 et seq.

[264] See further Centre on Regulation in Europe (CERRE), *Making Data Portability More Effective for the Digital Economy*, p. 42 et seq.

standardised APIs have to be developed as key prerequisite for efficient data transfers in practice.[265] On the legal side, standardisation processes for data exchange will have to be incentivised and covered legally (in particular in regard to competition law rules and practice).

3.4. Summary

The existing acquis communautaire already provides for a comprehensive legal framework for protecting the interests of the data holders – particularly by means of the database sui generis right and trade secret protection. At the same time, it safeguards the interests on the demand side by expressly granting data access and use rights in certain cases (e.g. GDPR, certain contractual instruments, sector-specific regulation), by sanctioning anti-competitive behaviour (Art. 102 TFEU) and by generally allowing for data transactions on contractual basis.

On the data holders' side, data collections can be protected (in certain cases) through the database maker's sui generis right or (more generally) as a trade secret. Whereas the Trade Secrets Directive provides a sufficiently flexible instrument (with only certain, mostly more practical contract and enforcement related shortcomings), the database sui generis right as foreseen in the Database Directive has the potential to aggravate access problems and to intensify de facto control over data. Due to its broad scope, it can in principle be invoked by the rightholder against access and portability rights – even though in practice the sui generis right might only have rather limited impact. In particular, there is significant legal uncertainty in regard to core elements of sui generis protection, such as the distinction between collection and creation of data, the notion of 'substantial part' and other.

Access to and portability of individual-level use data (first case group) is provided for personal data primarily through Article 20 GDPR and for non-personal data in the context of B2C contracts for the supply of digital content or digital services through Article 16 (4) Digital Content Directive. For business users so far no general data access or portability rights exist, unless foreseen in certain sector specific regulation. Apart from that, access to co-generated data is currently not granted in relation to service providers other than gatekeepers (by the proposed Digital Markets Act). General competition law, namely Article 102 TFEU, may apply where refusing access to data amounts to an abuse of a dominant position. Horizontal data access of competitors to complete sets of aggregated data necessary for workable competition in aftermarkets, complementary markets or even in the products or services market of the data holder (second case group) is hitherto primarily governed by general competition law.

In light of the existing legal framework and the recent developments in practice, law and policy we have identified need for action. First, the Database Directive and the database sui generis right are in need of reform. The conditions of protection – most importantly for machine-generated data (IoT, but also certain services) – have to be specified in order to reduce legal uncertainty. In addition, the exceptions and limitations should be revised as the sui generis right's limitation to the use of substantial parts and the existing limitations do not suffice for facilitating the re-use of data in the identified case groups of justifiable access to data. Furthermore, the allocation (ownership) of the database sui generis right, the term of protection, and the interface with national unfair competition

[265] See Centre on Regulation in Europe (CERRE), *Making Data Portability More Effective for the Digital Economy*, p. 86; cf. Deloitte, *Study on emerging issues of data ownership, interoperability, (re-)usability and access to data, and liability*, p. 139

instruments in some Member States law should be put under revision. As one remedy we have inter alia proposed to introduce a compulsory licensing regime for certain cases.

As regards the relation of data access and use rights to trade secrets protection, a more nuanced approach is necessary. The protection of trade secrets is justified insofar as incomplete information is a substantial condition for functioning and competitive markets, where such trade secrets concern market information or other information on the very parameters of competition. Beyond that (e.g. technical know-how), trade secrets protection serves the purposes of reducing transaction cost (inefficient factual protection measures) and fostering contractual sharing of information. On this basis, it has therefore to be carefully assessed whether and under which conditions access to (secret) information should be granted and whether, under which conditions (e.g. FRAND licences) and to what extent an 'access regime' should also cover the subsequent use of the respective information. In that regard, we have suggested that information on the very parameters of competition is even more sensitive than trade secrets relating to know-how and other information which do not directly relate to the competitive process as such.

The relation of access rights to the GDPR is an overall problematic issue. It is necessary to define the notion of personal data more specifically in sectors where access to industrial and technical data is predominantly concerned. This also entails providing for standards concerning technical and organisational measures for the reliable anonymisation of data and complementing this with at least a rebuttable presumption of sufficient anonymisation when businesses comply with such established anonymisation standards.

Moreover, enhancing data sharing and data portability in practice, largely depends on the technically, organisationally and legally effective feasibility. Therefore, laying down non-mandatory contractual model clauses for certain case groups is recommended to reduce transaction costs (in particular information costs also in order to raise the level of trust in particular of SMEs). Also, and as a general key element for any effective data transfer in the future, effective measures for enhancing technical and organisational interoperability have to be introduced.

4. PROPOSAL FOR A DATA ACT

KEY FINDINGS

We propose with regard to the **Data Act in general**,

- to **clarify and strengthen the role of private law enforcement**;
- to make the proposed public enforcement structures **optional** to the Member States and to streamline them, at best by a **one-stop shop approach** including a European 'meta-authority' for data related topics;
- to thoroughly assess the **coherence of the Data Act with the entire 'data package'** and the existing legal framework;
- to include provisions on the applicability of the Data Act in **multipolar settings** (e.g. data sharing networks);
- to **develop accompanying non-mandatory model contract terms**.

With regard to the proposed rules on **B2C and B2B data access, sharing**, **and use** we propose

- to **reconsider their broad scope of application and/or to critically evaluate the necessity of the mandatory character of the proposed system in B2B constellations** where no imbalance of the parties is present;
- to complement the central role of the user with a **regulation of the position of the data holders**;
- to assess whether access to data generated by the use of **services** is already comprehensively covered by the proposed Digital Markets Act and to consider the **extension of the scope of the new data access, sharing and use rights to certain larger (not purely data-processing, but data-driven) services** which are not gatekeepers under the comparatively strict thresholds of the proposed Digital Markets Act;
- to re-evaluate the exact extent of the principled **exclusion of inferred data**;
- to reconsider or at least to specify the conditions of the prohibition to use the respective data for developing a **competing product**;
- to consider whether the obligations to make data available set forth in the Data Act **could qualify as 'legal obligation' in the sense of Article 6 (1) (c) GDPR**, and, in the future, to consider further delineating the notion of 'personal data', at best by developing **technical and organisational standards for anonymisation** and by introducing a **rebuttable presumption** of anonymisation when the respective standards are met;

- to clarify that **FRAND 'licences' will cover necessary and justified use acts in regard to trade secrets**.

With regard to the **unfairness test for B2B contract terms** on data sharing we propose

- to specify that the fairness test does not apply to constellations in which a **micro or small business** is the imposer of a contract clause and
- to add the condition that a **gross imbalance** in the parties' rights and obligations arising under the contract must be the result of the unfair term.

With regard to **B2G data sharing** based on exceptional need we propose

- to reconsider whether the provisions should be **extended to small and micro-sized enterprises**.

With regard to the provisions on **switching between cloud and edge services** we propose

- to foresee an **exception for SMEs as providers**, at least for B2B relations;
- to revise the **relation to the proposed Digital Markets Act**;
- to **clarify the concept of 'functional equivalence'**.

With regard to the provisions on **interoperability** we propose

- to **extend the scope of the general principles** applicable to the operators of European data spaces to also guide future general standardisation processes in regard to cloud portability, data access and data sharing.

With regard to **Art. 35 on the database sui generis right** we propose

- to primarily 'refine' the wording of the provision in order to clarify that databases which fall into the scope of the Database Directive but which do not fulfil the substantive conditions of protection shall generally not be protected by other instruments of Member States' national law either, absent any additional objectives entirely unrelated to the investment protection objective of the Database Directive (**Union law pre-emption doctrine**).

With regard to an **ongoing and ex-post evaluation** of how legal instruments proposed in the Data Act are implemented and if they are efficient and effective, we propose

- to carefully **choose certain very specific, carefully limited and representative industry sectors** for possible evaluation of central instruments of the Data Act and possibly associated data collection as otherwise the very broad scope and generalising character of the Data Act will prevent the emergence of conclusive results.

We will now evaluate the Commission's proposal for a 'Regulation on harmonised rules on fair access to and use of data (Data Act)'[266] based on the need for action which we have identified in light of the existing legal framework (3.) and the recent developments in practice, law and policy (2.). We will start with some general remarks (4.1), before we will analyse in detail the key topics addressed in the proposal: the provisions on access for users of IoT products and sharing upon request by a user with third parties (4.2), the provisions on unfair contract clauses in B2B data sharing contracts (4.3), B2G data access in case of exceptional need (4.4), switching between cloud and edge service providers (4.5), unlawful third party access to non-personal data held in the Union (4.6), interoperability and standards (4.7), the implementation and the enforcement of the proposed measures (4.8) and the provision concerning the database sui generis right (4.9).

In line with the requested scope of this study, in our analysis of the proposed Data Act we will emphasise the aspect of 'data sharing', the newly proposed conditions and the necessary balance with relevant intellectual property rights, trade secrets, contract and data protection law. Furthermore, we will primarily focus on the subjects in regard to which we see room for improvement.

4.1. Introduction and general remarks

The Data Act constitutes an ambitious project and a courageous policy decision with the objectives to open certain markets related to the IoT and cloud sector, define explicit provisions for data sharing on contractual basis as well as reduce technical barriers and allow data access in exceptional situations. In order to establish 'harmonised rules on fair access to and use of data' it is a remarkable achievement that the Data Act proposes institutional, decentral structures (which from our viewpoint are typical for private law claims and should also be enforced accordingly, see below 4.1.3) for data access, use, sharing and portability, going thereby way beyond the current legal framework focused primarily on (more centralised) data and services governance. However, the proposed instruments, in particular because of their sweeping scope, require fundamental scrutiny in light of the involved impact on the principle of contractual freedom and certain 'fine-tuning' in regard to their details, also keeping in mind the objective to reduce market entry barriers for newcomers (or at least not to erect new barriers to market entry), in particular in the markets for IoT

[266] Proposal of 23 February 2022 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 (hereinafter 'Proposal for a Data Act'), Explanatory Memorandum, p. 9.

products and cloud services. Our analysis therefore aims at indicating potentially problematic points in order to analyse them thoroughly.

4.1.1. Comprehensive harmonisation and coordinated enforcement

To achieve the aim 'of ensuring fairness in the allocation of value from data among actors in the data economy and to foster access to and use of data'[267] it seems indeed necessary to choose the instrument of a 'Regulation' in order to guarantee a harmonised framework in the Union. For the same reason, i.e. because a comprehensive harmonisation and adequate legal certainty is key for being able to reach the objectives pursued by the Data Act, it has to be examined thoroughly and for all proposed instruments whether the enforcement by different competent authorities on different levels (Member States – EU) might put in danger the envisaged harmonisation effect (see further below 4.8). This should not only be considered for the Data Act but for the entire 'data package' comprising the the proposals for a Data Governance Act, Digital Markets Act, Digital Services Act plus the AI Act and even the existing data-related legal framework such as – most notably – the General Data Protection Regulation.

Due to the Data Act's aim to regulate *data markets*, it should be put under scrutiny whether competition authorities or at least other established *regulatory* authorities are more suitable as competent authorities than, for instance, data protection authorities or statistical offices of the Member States. As already shown above (2.2.2), granting rights to access to and use of data (both, personal and non-personal data) is in many ways highly interlinked with competition law and regulation. The rationales of general competition law can further serve as valuable guideposts for a specification of the Data Act as well as the interpretation of other instruments of Union Law (namely the Database Directive and the Trade Secrets Directive) which will be affected by and will have to be aligned with the application of the newly proposed provisions of the Data Act. They are also helpful in specifying instruments such as FRAND licences and concepts such as 'competition with the original product'. By contrast, data protection law and its enforcement are hitherto rather based on a fundamental rights approach. Even though the Data Act adopts certain regulatory techniques and principles used in the GDPR and applies them to non-personal data, the GDPR in itself cannot serve as a model as it centrally expresses and protects the data subjects' fundamental right to protection of personal data. Whereas positive effects of certain of the GDPR's provisions on free movement of data and the freedom of competition are undoubtedly present and expressly intended to be of equal importance, in hitherto practice such competition enhancing effects have proven to be at best rather a reflex in the overall context of the GDPR's personal data protection-oriented conception and enforcement. Due to these considerations, we would propose to allocate the competence for the public enforcement of the obligations set forth in the proposed Data Act either to the competition authorities itself or at least to another regulatory authority.

Further, and as a general recommendation, it should be considered to consolidate the competent authorities in the context of the different above-mentioned instruments and to introduce both, a network for cooperation and information exchange and also a meta-authority[268] as a 'one-stop shop' clearing house on the level of the European Union, where relevant applications, notifications, impact assessments, approvals, orders etc. should be concentrated. Ideally, this would prevent a

[267] Proposal for a Data Act, Explanatory Memorandum, p. 2.

[268] Weizenbaum Institute, *Position Paper concerning Data Act – Inception Impact Assessment*, p. 12. Cf. also Graef, I. and Prüfer, J., *Governance of Data Sharing: A Law & Economics Proposal*, p. 10 et seq.

fragmented administrative practice, foster legal certainty, and reduce administrative and other transaction costs.

Parallel to the argumentation brought forward in the context of the proposed Digital Markets Act (see above 3.1.7), in that context it should also be considered to base the Data Act therefore not solely on Article 114 TFEU but possibly also on Article 103 TFEU. Unlike the Digital Markets Act, the Data Act is a sector-specific regulation which does not contain genuine competition law elements or instruments, but, as described already, even such sector-specific regulatory approach can show a significant contextual closeness to certain concepts and instruments of competition law and other regulatory sectors. Also, express acknowledgement of the existing contextual relation to competition law would – first and foremost – allow to make use of the established enforcement and cooperation network of the national and European competition authorities (see above 3.1.7 and below 4.8.1).

4.1.2. General overlap problems and coherence of legal instruments

As a second remark concerning the planned instruments of the 'data package' and the existing legal framework relevant for data access and use (above 3.1), the relation between the different instruments, their purposes and their content needs to be clarified. If overlap issues remain unsolved or unclear, they will be a major factor causing legal uncertainty and opportunistic behaviour in the upcoming years.

In the current proposal, most of these overlap and consolidation issues are addressed by 'without prejudice'-clauses which reflects the typical approach to this problem in EU law.[269] For some of the overlaps this might indeed be an adequate solution, in particular where the scope and objectives of the concerned instruments can be clearly separated or do not really overlap.[270] However, in regard to certain other overlaps, such as the overlap with personal data protection (and possibly, in the future, also e.g. with the envisaged AI Act), such 'without prejudice'-clauses tend to obscure the fact that partly conflicting objectives have to be accommodated with each other, thereby striking a proportional balance between the involved fundamental rights and interests. This need for a proportional balance, at the same time guaranteeing that the essence of the separate involved fundamental rights is not affected in the balancing process, should therefore be addressed in a more transparent way in order to give the CJEU at least some further methodological guidance with regard to the necessary consolidation and accommodation of the different relevant instruments of Union law and their partly differing objectives. The balancing of interest clauses contained in the GDPR, e.g. Articles 15 (4) and 20 (4) GDPR according to which the data subject's access and portability rights 'shall not adversely affect the rights and freedoms of others', can serve as a first example in this regard.

Considering for instance the proposed access and sharing rights in the context of IoT products, a comparable weighing of interest might allow to find adequate solutions with regard to the relationship with protected trade secrets and in regard to affected personal data. However, one may

---

[269] See inter alia Recitals 7 et seq. or Article 24 (1) Proposal for a Data Act.

[270] The proposals for the Digital Markets Act and the Data Governance Act are not addressed by such clauses, likely because they are designed to *complement* the Data Act, see Proposal for a Data Act, Explanatory Memorandum, pp. 4 et seq. Concerning the Digital Markets Act, this approach seems reasonable as the current proposal for the Data Act is designed not to apply to 'services' which are subject to the Digital Markets Act (see further on this distinction, 4.2.1.c.ii). If the scope of the Data Act extended to data generated by 'services', the relation to the Digital Markets Act would however have to be clarified.

criticise that balancing of interest clauses or comparable open 'standards' inevitably lead to even increased legal uncertainty. Therefore, even further specification and guidance on how to accommodate the different instruments of Union law and affected subjective rights with each other, e.g. by making use of an interpretation of existing general clauses in consistency with the overall *acquis communautaire* and carefully aligning the different concepts and instruments, is strongly recommended. These remarks are of a general nature at this point and we will focus more detailed on particular overlap, consolidation and balancing issues in the following.

4.1.3. Private law enforcement and need for specification

In general, the Data Act is characterised by broadly formulated standards ('general clauses') and many new legal concepts and terms. These provisions, terms and concepts will have to be further clarified and specified in the upcoming years. Since the Data Act assigns an important role to bilateral (contractual) agreements as a private law institution, the 'task' to specify the proposed provisions should centrally lie with private law courts, thus should be addressed within private law enforcement, and not by public authorities as part of public enforcement. It should be considered to lay down rules on this prevalence of private rights and litigation and, more generally, on the substantive and procedural relationship between the public enforcement mechanisms, foreseen in Articles 31 et seq.[271], and private litigation as the presumptive main pillar of putting this new institutional framework into practice.

4.1.4. The role of contract law and need for respective model or standard contract terms

Within the Data Act and its instruments bilateral contractual agreements between the relevant actors serve as essential basis. However, model contract terms for their concrete realisation are – still – lacking (see already above 3.1.8.b). The Data Act touches upon this issue solely in Article 34 according to which 'the Commission shall develop and recommend non-binding model contractual terms on data access and use to assist parties in drafting and negotiating contracts with balanced contractual rights and obligations'.

As a consequence, the legal uncertainty when drafting contracts – inter alia precisely for the sale/rental/leasing of a smart device, for B2B data sharing, for cloud/edge services and the involved intricate IP- and competition law related issues – remains unchanged for the moment, just as the significant information and transaction costs. The lack of model contract terms will become even more problematic than before since the proposed access and use rights in the context of data generated by IoT products or related services (Articles 4 et seq.) build on the assumption that the user has to 'authorise' any processing of non-personal data by contractual agreement (Article 4 (6), see further below 4.2.3.e), thus resulting in tri-lateral relationships, in some situations even where hitherto a bilateral agreement would have been adequate. Clearly, a general principle of good faith, certain cooperation duties, and basic procedural guidelines for balancing the involved interests, legal and factual positions in regard to the access to and sharing of data will be required in order to make the contract-based implementation of the Data Act's access- and sharing-rights system effective in practice.

[271] Art. without further reference are articles of the Data Act Proposal.

Moreover, the entire network aspect of the relevant data access and sharing scenarios (in particular also concerning needs for aggregated data by multiple companies of a large number of different users and respective problems of contractual design and enforcement in larger, multipolar networks) is currently not addressed at all. Although this does not seem to be the central objective of the obviously more sector-specific approach in the Data Act anyway, even in regard to the specifically envisaged IoT scenarios, the current emphasis on bilateral contracts leaves aside that many data sharing scenarios, for instance data sharing networks or cooperation, involve multiple actors as users/customers, data holders and data seekers. Thus, for instance in many situations multiple data holders (original equipment manufacturers, component producers, AI services) and data users (AI services, other related services etc.) will collect or require only very specific, well-defined parts of the data stream of a given original product (as the sheer amount of the collected data, e.g. the huge amount of data which a connected car 'produces' in each and every minute, currently prevents central collection or use on a broader scale). Therefore, it has to be clarified whether and to which extent the provisions proposed in the Data Act should apply in such more complex multipolar network constellations. This is of particular importance not only for the access and sharing rights for data generated by IoT products, but also for the 'fairness test' for B2B data sharing contracts which is obviously not designed to deal with multipolar contract negotiations and networks. In addition, further aspects such as allocating the sui generis right or trade secrets by means of contractual agreement (see above 3.2.2.b.iv and 3.2.4) remain unsolved.

4.1.5. Relation to the GDPR and the notion of personal data

As regards the processing of personal data, it has to be highlighted positively that the Data Act takes into account the entire 'toolbox' of the GDPR by referring to any legal basis foreseen in Article 6 GDPR (or Article 9 GDPR) instead of relying solely on the data subject's consent. Requiring consent in the sense of Article 6 (1) (a) GDPR – or under the even stricter standards of Article 9 (2) (a) GDPR – in each case would render the data access and sharing rights rather useless due to the high standards, legal uncertainty and practical difficulties, in particular in regard to dynamically involving use scenarios as well as for uses based on relevant sensitive data. In this context it should always be borne in mind that the GDPR expressly pursues two – equally important – objectives consisting in the protection of natural persons with regard to the processing of personal data *and* the free movement of personal data.[272]

In the context of the proposed Data Act, the immensely broad definition of personal data in Article 4 (1) GDPR – which at the same time entails a *negative* definition of *non-personal* data – should be put under scrutiny. Large parts of the data processed in the data-driven economy relate (at some point) to an identifiable natural person or at least cannot clearly be distinguished from non-personal data. The same applies for data generated by IoT products: Location data (e.g. connected cars), use data (e.g. smart home devices) or search queries 'asked' to a virtual assistant will certainly qualify as personal data in the sense of the GDPR. The proposed Data Act seems to somehow transcend the so far strict distinction between instruments for personal and non-personal data as it imposes rights of the user and obligations of the data holder that show substantial similarities to the protection of personal data (to a certain extent aligning the instruments for personal and non-personal data). Thus, a data holder has to agree with the user on the processing of both personal and non-personal data. At first sight, this seems to solve the problem of the hitherto often very difficult (and data

[272] This is already stated by the title of the GDPR; see furthermore Article 1 GDPR and Recital 13.

protection-friendly) distinction between personal and non-personal data. However, the Data Act at the same time strictly refers to the GDPR as regards the definition of personal data and the conditions of lawful processing of such data. This neglects that in order to make a system of IoT data access and data sharing work effectively in practice, it might be necessary to fundamentally specify the scope and impact of the GDPR in the sector, i.e. to at least consider amendments to the definition of personal data in such scenarios in a way which is in line with the objective to improve the free flow of sufficiently anonymised or manifestly publicly available data, as well as to specify and clarify the specific possibilities to balance the legitimate objectives behind the Data Act with the fundamental right to protection of personal data by interpreting the respective heads for lawfulness of processing in Article 6 GDPR in accordance with the legal duties set out in the Data Act. We will deal with some of these issues in further detail below 4.2.3.d.

Apart from these detailed proposals, one aspect would be central to improve the conditions for businesses in the internal market in that regard. As the Data Act aims at reducing the practical and technical barriers for data sharing by introducing standards for interoperability, smart contracts and other relevant technical features, in the context of the GDPR this should also be an occasion to further implement legally reliable technical (and organisational) standards for the sufficient anonymisation of data (see above 3.3.3).

4.1.6. Overlap with IP rights and protection of trade secrets

The proposed provisions of the Data Act consequently and rightly focus primarily on potential overlaps with the protection of information as trade secret (particularly Chapter II, III) and with the sui generis right of database makers (Article 35). With respect to intellectual property rights other than the sui generis right, the Data Act does neither contain specific provisions nor should it typically affect these rights.[273] General copyright law (see above 3.2) and patent law are indeed of rather marginal importance for the protection of data collections. Nonetheless, particular case groups in which, for instance, copyright protection of a database work (due to its creative structure)[274] or patent protection concerning certain encryption or compression processes[275] might play a role, seem possible. However, the definition of copyright's conditions for protection ('work') and the scope of the exclusive rights seem to offer sufficient flexibility for addressing potential overlaps adequately.[276] Similarly, in Member States' patent law, case law on the scope of protection and enforcement in regard to process patents and direct products of processes, can and should be handled in a way to avoid substantial interference with the objectives of the Data Act and the entire 'data package'. As a result, an explicit exception or limitation for potential overlaps with intellectual property rights other than the sui generis right and respective clauses on the necessary balance with trade secrets protection does not seem necessary. As far as the Data Act goes, the remaining systematic frictions with other branches of IP law can be handled within the respective IP rights by interpreting them in accordance with the objectives behind the 'data package'.

---

[273] According to the Explanatory Memorandum (p. 5), the Proposal for a Data Act should not affect intellectual property rights other than the sui generis right.

[274] Cf. constellation in the *IMS Health* case, CJEU, judgment of 29 April 2004, *IMS Health v NDC*, C-418/01, EU:C:2004:257.

[275] In this direction German Federal Supreme Court (BGH), judgment of 21 August 2012, *MPEG-2-Videosignalkodierung*, X ZR 33/10; German Federal Supreme Court (BGH), judgment of 27 September 2016, *Rezeptortyrosinkinase II*, X ZR 124/15.

[276] Cf. Leistner, M., Antoine, L. and Sagstetter, T., *Big Data,* p. 438. See as general example for resolving overlaps between copyright and design law by interpreting the conditions for protection, CJEU, judgment of 12 September 2019, *Cofemel v G-Star Raw*, C-683/17, ECLI:EU:C:2019:721.

4.2. Business to Consumer and Business to Business data sharing (Chapter II & III)

Chapter II and III (Articles 3–12) implement a new regime of access and use rights for the user of IoT products and related services but also for data sharing with third parties as far as this is requested by the user. The user's access and use right is provided for in Article 4, the right to share data with third parties in Article 5. The following Articles specify the data holder's obligations (Article 6), their scope (Article 7) and the conditions for making data available to third parties (Articles 8–12). First, we will address the general scope and objective of the proposed provisions relating to 'data generated by the use of products or related services', before we elaborate on them in detail.

4.2.1. General scope and objective

a. General regulation for the IoT sector and institutional regulatory objective

The provisions proposed in Chapter II and III granting access and use rights for users and the right to share data with third parties in regard to data 'generated' by IoT products and related services are designed to constitute generally applicable, *basic rules for all sectors* in this field.[277] Due to this horizontal character covering the entire 'sector' of IoT products, the proposed provisions, on the one hand, have a very broad scope of application – from industry to private use of connected products (B2C and B2B alike, see further below b.). On the other hand, in regard to the relevant data, the scope of the Data Act is limited to 'data generated by the use of products or related services' and thus does not substantially cover any inferred or derived data (see further below c.iv) and the access to, use and sharing of these data is limited to uses which do not compete with the IoT product from which the data originate (see further below 4.2.3.c).

Consequently, these provisions can neither be consistently construed as addressing specific situations of abuse of dominant market positions (or other situations of specific market failure) nor as addressing specific situations of information asymmetry, imbalances in negotiation power (or other situations of specific contract failure). This is because under the perspective of situation-specific market failure or situation-specific contract failure, the scope and structure of the provisions would be at the same time both, too broad as well as too narrow. The scope would be too broad as these provisions obviously also apply in situations where no information or market power asymmetry can be identified at all. This is because, in particular in B2B settings, the user of the IoT product might as well be better informed and more experienced than the IoT product provider and data holder, and might also have a relatively stronger market position resulting in a relatively stronger negotiation position. In such a setting, broadly applicable, sector-wide mandatory provisions on data access and sharing cannot be justified as a corrective for a specific situation of market or contract failure. On the contrary, in some of these situations they might outright interfere with efficient, contract-based allocation of data, as because of their mandatory character, they prevent any reservation of data-related aftermarkets based on factual data control or contracts, even in situations, where this would be the efficient solution and would therefore benefit both parties to a respective contract.[278] At the same time, the scope would be too narrow, as we have identified

[277] Proposal for a Data Act, Explanatory Memorandum, p. 5.

[278] In B2B relationships, situations in which – due to particular investments etc. – a limitation of the user's access and use rights (by means of an agreement) may seem reasonable to both of the parties are undoubtedly conceivable, see Schweitzer, H. and Peitz, M., 'Ein neuer europäischer Ordnungsrahmen für Datenmärkte?', *Neue Juristische Wochenschrift*, 2018, p. 280.

situations of potential market failure in regard to the access to aggregated data, and, namely structured data, i.e. contextualised, standardised data, as the genuine main bottleneck for the development of many data oriented services at the moment (see above 2.1.1). However, for such situations, the new provisions do not really provide a comprehensive remedy, because their field of application is limited to volunteered and observed data (see further below c.iv) and their fundamental structure is oriented towards the access to and sharing of individual-level data (which at best indirectly and inefficiently helps to remedy situations where access to aggregate, contextualised datasets would be necessary and justified).

Instead of remedying specific situations of market or contract failure, the newly proposed provisions on data access, use and sharing in the Data Act are based on the general assumption that access to and use of IoT data in order to provide new products or services (in particular, but not only, maintenance, repair and other aftermarket services or products) will liberate aftermarkets and other new markets through the provision *and* commodification of data access rights, and will thus, in their total effect, create more benefits through enhanced dynamic efficiency than costs[279] (through the undoubted interference with static efficiency in certain situations, in particular B2B situations). According to Recital 14, this can be based on the assumption that the respective 'data are potentially valuable to the user and support innovation and the development of digital and other services protecting the environment, health and the circular economy, in particular through facilitating the maintenance and repair of the products in question'. The objective is thus to provide an institutional framework for the development of new markets, in particular in regard to new products or services in markets related to the distribution of IoT products, through opening and institutionally structuring hypothetical or actual upstream markets for the access to the necessary data generated by such products.

This new regulatory approach, which goes way beyond the existing, comparably problem-specific approaches in competition and consumer protection law, is at the same time limited in scope to IoT products and related (after)markets as well as in regard to upstream markets for (volunteered or observed) data generated by the use of such products. Thus, while the regulated sector (use of any IoT product, B2C and B2B) is very broad and unspecific (*broad horizontal field of regulation*), the affected data categories (only volunteered and observed data as such) as well as the statutorily enabled uses (use for developing competing products is expressly excluded) are remarkably limited (*limited vertical depth of regulation*). However, even in light of these crucial limitations, it has to be borne in mind that the sectors in which data-collecting IoT products are used, vary widely, and thus, the conditions on the relevant markets, the relationship between the actors, their respective interests, and the amount and categories of the co-generated data differ significantly. Also, the aspect of possible new barriers to market entry (or at least chilling effects) for original producers which have not yet implemented IoT components in their products at all should not be lost out of sight. General competition law sanctions *market dominant firms* for exclusionary conduct by leveraging their dominance on an (actual or hypothetical) primary market to a secondary market, but which might comprise situations where the new product or service (by the licence seeker) is in direct competition with the product or service of the incumbent. By contrast, the Data Act might be interpreted as a decision for *generally* opening (hypothetical) markets in the IoT sector through a *general ex-ante (market design)* approach, since from the viewpoint of the Commission the existing,

[279] Commission Staff Working Document, *Impact Assessment Report*, Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), SWD(2022) 34 final, p. 43 et seq.; Deloitte and others, *Study to support an Impact Assessment on enhancing the use of data in Europe*, p. 270 et seq.

competition law-based *case-by-case* analysis has turned out not to be effective enough to generally foster the development of certain data-driven markets. Following this assumption, it would however also have to be shown, whether a generalised *mandatory* law framework is indeed required to reach this objective throughout the entire sector, whether solely opening *secondary* markets (by excluding data access, use or sharing in order to *compete* with the data holder) is sufficient and in particular, how such secondary markets shall be defined and delineated from situations of (direct) competition with the data holder in borderline cases. In that latter regard, the Data Act remains remarkably cautious, thus at the same time significantly limiting the impact of this new regulatory instrument for crucial case groups.

From our viewpoint, all this has three main consequences for our analysis which result in two main policy recommendations:

First, given the diversity of their field of application, the new provisions have to be evaluated with particular attention to their *flexibility*, the use of standards, and the question which institutional players shall specify these standards in the future as this will be crucial for the necessary balance between flexibility through the use of open ended standards and fostering sufficient legal certainty through the specification of these standards in case law (this particularly also concerns the question of private and/or public enforcement and their relationship with each other). Secondly, it has to be kept in mind that none of these new provisions should be designed, construed or applied in a way which puts disproportional *new cost burdens on newcomers* in the very markets the Data Act intends to open and incentivise (this particularly at least concerns necessary lenience in regard to SMEs as well as – again – the issue of efficient enforcement which might be endangered if overlapping, multi-institutional enforcement causes significant additional administrative and information costs, e.g. because of resulting legal uncertainty). In fact, as a *policy recommendation*, these two aspects lead to a need to *reconsider the very broad scope* of the proposed mandatory framework and, in particular, to re-evaluate whether *mandatory rules* are indeed needed in those B2B-constellations, where no manifest imbalance exists between the parties to the contract.

Thirdly, one has to remain aware that the *access problems*, which have been identified in the first part of this study (see above 2.), go way beyond the specific field of certain data co-generated by IoT products and the opening of related aftermarkets for products or services which are not in direct competition with the data generating IoT product itself. This is especially true for access needs of competitors to complete datasets for competing in secondary markets (which might include inferred data), and access to large aggregated datasets (e.g., training data) of big data conglomerates for innovation purposes (second and third case group) which might even lead to products or services which *are* in direct competition with the data generating product or service. Due to the strict exclusion of 'services', data generated by the use of (online) services or platforms are not covered by the proposed Data Act. This sector is therefore hitherto only covered in the 'data package' by the proposed Digital Markets Act, albeit limited to data held by gatekeepers (i.e. the GAFAM companies plus a handful of other gatekeeper platforms) and to specific market situations. Therefore, it will be necessary to design and construe the new provisions in the Data Act in a way which allows them to at least indirectly contribute to the solution also of some of these (partly related) data access problems. Also it has to be kept in mind that the above-mentioned access problems, in particular in regard to aggregated, contextualised or standardised data and in regard to services, might need to be addressed in the future, going beyond the limited data related rights vis-à-vis Big Tech companies in the proposed Digital Markets Act. In sum, this leads to the *policy recommendation* to reconsider the limitation of the scope of the Data Act's proposed access and sharing regulation to IoT-products and related services only, to re-evaluate the exact extent of the

principled exclusion of inferred data[280] as well as to reconsider the principled requirement of non-competing use.

b. Equal rights for B2B and B2C relations and essential role of the user

If one accepts the regulatory objectives outlined in the preceding part as being legitimate and consistent in the first place, nonetheless, in particular for B2B constellations it also needs to be justified *why the user should be in a central role*. Whereas protecting *personal data* by means of strong subjective rights (as provided by the GDPR) is mandated by the fundamental right to protection of personal data, the need for allocating mandatory access, use and sharing rights in regard to *non-personal* data to the user as suggested by the Data Act, is less self-evident (see further below).

Allowing access to and use of data generated by IoT products and related services for B2C relations can be seen as an expression of guaranteeing data sovereignty and 'empowering' of private consumers in regard to perceived information asymmetries or other reasons for an assumed weaker bargaining position of private consumers.[281]

However, in B2B constellations, such allocation of non-personal data to the customers/users of IoT devices needs genuine justification. As we have explained, in B2B constellations, where the customer/user is not an SME, such mandatory allocation of data access, use and sharing rights, cannot across the board be justified by the identification of specific situations of market or contract failure[282] – this would at best be possible for SME users vis-à-vis large IoT companies or for certain very specific sectors where empirical data clearly suggest the general actual or potential existence of such situations. The Data Act goes beyond this, covering all B2B relations alike, where IoT products are used by businesses on the basis of sales, rental or lease contracts. Thus, it seems that the mandatory allocation of data access, use and sharing rights to *business users* of IoT products is based on the perceived co-initiative and co-investment of such business users in the *generation* of the resulting use generated data through their actual use.[283] As for the allocation of *exclusive rights* in such data, it has been decided by the CJEU in the context of the database sui generis right, that the mere generation of data in the course of another main business activity (i.e. as a spin-off of such a main business activity), shall *not* give rise to exclusive rights based on such more or less incidental *generation* of data.[284] As for B2B situations under the Data Act, the crucial (and somewhat different) question is whether the contribution to the generation of data through use of IoT products in the context of another main business activity, should at least give rise to certain limited and *non-exclusive access, use and sharing rights for the user*.

Certain systematical elements of the existing EU *acquis communautaire* in digital IP law point (non-conclusively) in that direction: In particular, the Computer Programs Directive[285] as well as the

---

[280] See also Kerber, W., *Governance of IoT Data: Why the EU Data Act will not fulfill its objectives*, p. 12.

[281] Proposal for a Data Act, Explanatory Memorandum, p. 13.

[282] Similarly, Kerber, W., *Governance of IoT Data: Why the EU Data Act will not fulfill its objectives*, p. 25.

[283] Cf. Recital 6 Proposal for a Data Act. Further on the aspect of 'co-generation' Principle 18 and the flexible factors proposed therein, *ALI-ELI Principles for a Data Economy – Data Transactions and Data Rights*.

[284] CJEU, judgment of 9 November 2004, *British Horseracing Board v Hill*, C-203/02, EU:C:2004:695, paragraphs 30 et seq.; CJEU, judgments of 9 November 2004, *Fixtures Marketing v Oy Veikkaus,* C-46/02, EU:C:2004:694; *Fixtures Marketing v Svenska Spel,* C-338/02, EU:C:2004:696; *Fixtures Marketing v Organismos prognostikon,* C-444/02, EC:C:2004:697.

[285] Articles 5 and 6 Computer Programs Directive, see further 3.3.1.a.ii.

Database Directive[286] foresee certain *mandatory minimum use rights* for the *lawful user* of a computer program or a database, e.g. for use acts to correct errors, making backup copies, observe, study or test certain elements of the program or the database; however, technically these so-called 'rights' only constitute *exceptions* from the exclusive protection of the computer program or database rights holders and therefore mere '*freedoms*' of the user as opposed to genuine (and to a certain extent 'tradable') access, use and sharing *rights*. Nonetheless, one might argue that this concept of certain minimum mandatory rights for lawful users of certain digital products can serve as a contextual starting point for respective new minimum rights of users of IoT products which might comprise certain rights in regard to the access to, use of and sharing of data generated by the use of such products, in particular if this reflects the reasonable expectations of the users.[287]

Whereas certain contextual elements in the *acquis* can therefore serve as a tentative model for the access, use and sharing rights for business users in the Data Act, the crucial question remains whether the initial allocation of such rights to the *users* of the devices is efficient, when assessed in light of one of the main objectives of the Data Act, i.e. to create new markets for such data as a necessary precondition for the offer of new products and services in aftermarkets related to the originally distributed IoT product or its use. To answer this question, it will have to be considered, whether the users of such devices are sufficiently informed and incentivised to *actually make use of their new rights*, in particular also to share (and effectively market) them. In a rather limited field, i.e. the provision of specific new or at least cheaper or better services in aftermarkets, one might assume that the users as prospective customers of such services, might indeed be the best informed agents and might have sufficient incentives in order to initiate the necessary sharing of data by the data holder. At the same time effects, such as switching costs and inertia bias as well as the associated transaction costs, might well reduce the incentives of the users to effectively initiate data sharing. To make this envisaged regulatory system work, first, the relevant provisions of the Data Act must allow for broad, non-static and transferrable sharing claims (see below 4.2.4.a). Secondly – and more importantly – it will have to be considered whether the central (and to a certain extent 'proto-exclusive') role of the *users* in regard to *initiating* upstream data sharing is indeed as such sufficient to effectively foster the emergence of dynamic and diverse new data markets as a precondition of new data related products or services (see below 4.2.3.e).[288]

In this context, it should also be kept in mind that the very generating, obtaining and observing of data generated by the use of a product or related service at the same time requires substantial ex-ante and continuous organisational, technical and financial efforts *by the data holders*. Also, in many situations, the data holders might be in a better situation to assess, negotiate and implement efficient data contracts, whereas the users' respective initiative and role seem less central and functional in that regard. In order to effectively incentivise data sharing, the role and legal as well as practical position of the data holders (IoT producers and related companies) should therefore be equally taken into consideration, when allocating rights to share such data on a non-exclusive basis with third parties (see below 4.2.3.e).

[286] Article 8 Database Directive.

[287] Cf. Leistner, M., Antoine, L. and Sagstetter, T., *Big Data,* pp. 65 et seq., p. 444 et seq.

[288] Cf. also Kerber, W., *Governance of IoT Data: Why the EU Data Act will not fulfill its objectives*, p. 2 et seq.

c. 'Data generated by the use of products or related services'

Articles 3 et seq. apply to all 'data generated by the use of products or related services'. As these provisions are tailored to the 'IoT-specific' approach of the Data Act, this scope of application is in principle consequent.

i. Products or related services

According to Article 2 (2), a product is defined as a 'tangible, movable item, including where incorporated in an immovable item, that obtains, generates or collects, data concerning its use or environment, and that is able to communicate data via a publicly available electronic communications service and whose primary function is not the storing and processing of data'.

In line with the definition of 'goods' in Article 2 (5) (a) of the Sale of Goods Directive, the Data Act adds as particular requirement the ability of the product to obtain, generate or collect data and to communicate such data. Pursuant to Recital 14, relevant products might be for instance vehicles, home equipment and consumer goods, medical and health devices or agricultural and industrial machinery.

However, it should be verified why the definition is limited to a communication of data via *publicly available* electronic services. As on the one hand it seems possible that data is – or at least could prospectively be – transmitted by means of a private communication service and, on the other hand, no evident reason for such exclusion is apparent, the definition should be broadened to cover *any* electronic communications services or otherwise the differentiation should be explained properly.[289]

The exclusion for products 'whose primary function is not the storing and processing of data', thus, products that are not primarily designed to 'display or play content' (see Article 15) is persuasive and appears to be workable in practice as the purpose for excluding respective products becomes sufficiently clear for an interpretation.

The definition of 'related service' in Article 2 (3) is based on the definition of 'goods with digital elements' in Article 2 (5) (b) Sale of Goods Directive. Recital 16 clarifies that consequently the contents of the sale, rent or lease agreement or the reasonable expectation of the user in light of the nature of the product taking into account public statements made by or on behalf of the seller, renter, lessor or certain other third parties is decisive for the inclusion of related services. To clarify the text of the Data Act, it should be considered to include this subjective-objective assessment perspective in the text of Article 2 (3) by adding the words 'according to the reasonable expectation of the user' at the end of that provision.

ii. Exclusion of data generated by other services

As we have explained above, the exclusion of services from the scope of the Data Act has a certain consistency, if the main objective of the act is a sector-specific regulation for the IoT sector. On the one hand, the Data Act has a remarkably broad scope for a so-called sector-specific instrument, given the variety of different existing and potential future IoT markets (which might still require

[289] Cf. also definition used by Drexl, J., *Data Access and Control in the Era of Connected Devices*, p. 28: 'This Study uses the term 'connected device' in a broad sense, namely, as all devices that (1) are connected with other things and persons through wireless or wired communication and (2) generate data'.

certain differentiations and qualifications), on the other hand, if the Data Act has to be understood as a sector-specific instrument in that sense, the exclusion of services, in particular internet services and platforms, is comprehensible.

Nevertheless, it should be put under scrutiny whether excluding data generated in the context of (online) *services*, is a convincing result in the overall context of the EU 'data package'. The proposed Digital Markets Act covers certain access and use rights in relation to online (platform) services. However, whereas the Data Act foresees access and use rights for *any* user and in relation to *every* data holder – except micro or small enterprises – wherever data generated by IoT products or related services are at stake, the Digital Markets Act provides certain access rights solely in relation to *gatekeepers*. As a result of the very high requirements for being qualified as a gatekeeper (Article 3 (1), (2) Digital Markets Act), the vast majority of online service providers is therefore not obliged to make data generated by the use of services available, even though they might have significant importance and market power in the European market.

The result (comprehensive access rights in the IoT sector vs. limited access rights in relation to gatekeepers for digital services) seems somewhat askew. To be sure, where online-services are directly based on a purely data processing business model, such services can be distinguished from the distribution of IoT products as they exclusively or at least predominantly recoup their investments by commercialising the very acquired data which justifies a different legal treatment. However, there are also many other services and platforms, which are based on different mixed business models, for which the factual ownership or commercialisation of incidentally acquired use or sales data are not central (e.g. even very large sales, booking, delivery or payment platforms or services), but which are data-driven in the sense that they profit in the markets from control over user data because of direct or indirect network effects[290], and which however do not reach the gatekeeper thresholds of the Digital Markets Act). For such services, the market situation might indeed be rather similar to the situation of IoT producers and users and it should be reconsidered why they should be excluded from the scope of the Data Act. At least the justification and impact of the exclusion of such services should be re-evaluated thoroughly, e.g. through a 'case study' looking at European service providers with data-driven mixed business models which do not qualify as gatekeepers but nonetheless play an important structural role on the internal market. As a result, it might be recommendable to extend the scope of the Data Act's data access, sharing and use provisions to such not purely data-processing, but data-driven services at least if they have a significant market share.

iii. The definition of 'user'

The 'user' of a product is defined as meaning any 'natural or legal person that owns, rents or leases a product or receives a services (sic!)'.[291] According to this definition, the user has to conclude – first – a contract with the seller, renter or lessor of the IoT product. The contracting party for the acquisition of the product does not necessarily have to be identical with the 'data holder' (Article (3) (2) (e)). We would suggest to extend the definition further to any 'lawful user' or person 'that otherwise lawfully uses' the product. As established above (3.3.1.a.ii), the concept of the 'lawful user' enshrined in general copyright law and the database sui generis right can serve as a contextual

[290] Argenton, C. and Prüfer, J., 'Search Engine Competition with Network Externalities', *Journal of Competition Law & Economics*, 2012, pp. 76 et seq.; Prüfer, J. and Schottmüller, C., 'Competing with Big Data', *The Journal of Industrial Economics*, 2021, pp. 968 et seq.; Graef, I. and Prüfer, J., *Governance of Data Sharing: A Law & Economics Proposal*.

[291] The spelling mistake 'services' should be corrected.

model leaving enough room for allocating access and use rights *for subsequent users* (e.g. in cases of resale of an IoT product or similar situations).

iv. Data 'generated by the use'

The rights set forth in Articles 4 and 5 cover 'data generated by the use of products or related services'. As Recital 31 specifies, this comprises actively provided (*volunteered*) or *observed* (*captured*) *data*. In contrast, inferred data are not covered by the Data Act.[292] At first sight, it could be argued that precisely inferred data are key tool for profiling of the user and should therefore be made available – at least to natural persons (B2C). However, profiling based on personal data is already sufficiently regulated by means of the GDPR.

The Data Act has a different objective as it points at opening (secondary) markets in the IoT sector. To be sure, access to inferred data (i.e. contextualised, standardised data) also would be very valuable and helpful in that regard.[293] But at the same time, such even broader access rights for a very large, very diverse sector, such as the entire IoT sector, would undoubtedly also have adverse effects on the market and the potential to hamper workable competition, e.g. by reducing incentives for investing in the further processing of data to acquire contextualised or standardised datasets of significant value. Therefore, while incentives for further investing in the contextualisation and standardisation of data and the production of versatile, high-quality datasets seem necessary, a general extension of the proposed Data Act's general access, use and sharing rights to inferred data cannot be recommended since this might even disincentivise necessary investment in that area. Nonetheless, the exact extent of the resulting exclusion of inferred data in the context of the definition of volunteered or captured (observed) data should be re-evaluated and the definition of volunteered and captured data should be specified and re-calibrated if necessary.

Continuous and real-time access to data generated by the use of the product or related service is generally covered by the rights of the Data Act, but solely 'where applicable', see Article 4 (1) and Article 5 (1). The Data Act does not provide a definition in which cases real-time access is 'applicable'. As part of the information duties before concluding a contract for the acquisition of a product, the user should be informed according to Article 3 (2) (b) 'whether the data is likely to be generated continuously and in real-time'. Limiting real-time access to cases in which the contractual agreement explicitly foresees continuous and real-time access appears too narrow, particularly in light of the access 'by design/default' principle (see immediately below). Since real-time access is of particular importance, e.g. for multi-homing, smart home applications or comparable services, and at the same time will be very costly and difficult to implement (in some cases the costs may even be prohibitive if the total amount of data were addressed), the need for continuous access to data ('where applicable') should be evaluated very precisely based on the particular product or related service and the *objective reasonable expectation of the user*. At least a respective Recital specifying the realm of continuous and real-time access should be added.

---

[292] See Proposal for a Data Act, Recital 14: 'The data represent the digitalisation of user actions and events and should accordingly be accessible to the user, while information derived or inferred from this data, where lawfully held, should not be considered within scope of this Regulation'.

[293] Kerber, W., *Governance of IoT Data: Why the EU Data Act will not fulfill its objectives*, p. 12.

4.2.2. Data access 'by design/default' and information duties (Article 3)

Article 3 (1) introduces the concept of data access 'by design' and 'by default' according to which the user of a product or a related service should be enabled to access data generated by the use 'easily, securely and, where relevant and appropriate, directly'. Article 3 (2) stipulates information duties that have to be fulfilled before concluding a contract for the purchase, rent or lease of a product or a related service. Both, the general principle set forth in Article 3 (1) and the information duties in Article 3 (2), show certain parallels to the GDPR.

Article 3 (1) appears to be rather a *general principle* than an enforceable obligation. However, when looking at the comparable principle 'privacy by design' and 'by default' set forth in Article 25 GDPR, this interpretation is not unambiguous: Even though the role of Article 25 within the GDPR is not completely clear[294] as apparent from Article 83 (4) (a) GDPR, it can be sanctioned as a 'real' obligation, inter alia by imposing administrative fines.[295] The Data Act does not elaborate on the question of enforceability. The sentence '[m]anufacturers and designers have to design the products in a way that makes the data easily accessible by default, and they will have to be transparent on what data will be accessible and how to access them',[296] might be interpreted as pointing in the direction of a 'real obligation'.[297] This in fact concerns public enforceability (as partly foreseen in Article 31 et seq.) as well as the relationship to EU and national contract law of the Member States, where such obligation might be understood as defining the conformity of the goods with the sellers', renters' or lessors' obligations under the respective sales, rental or leasing agreements. To avoid legal uncertainties in that regard, the meaning of Article 3 (1) (mere general principle which namely cannot influence the specification of conformity with a contract in Member States' contract law) should therefore be clarified at least in the Recitals to the Data Act.

The scope of the information duties seems reasonable and, in light of the assumption that any processing of non-personal data generated by the use of a product or related service, has to be based on a contractual agreement, even adequate. Since Article 3 (2) does not distinguish between personal and non-personal data and thus relates to data created by the use of a product or related service in general, where the user is a data subject, the additional information duties set forth in Articles 13 and 14 GDPR would have to be fulfilled (see also Recital 23).

4.2.3. Right of users to access and use data (Article 4)

a. General requirements

Article 4 stipulates '[t]he right of users to access and use data generated by the use of products or related services'. Pursuant to Article 4 (1) this right applies in cases in which the data is not already accessible for the user as a result of the data access 'by design and by default' principle (Article 3 (1)).

The data holder is obliged to make the respective data available to the user *free of charge*. That the *user* shall not incur any costs for getting access to the data generated by its use of a product or

---

294 See for instance Rubinstein, I. and Good, N., 'The trouble with Article 25 (and how to fix it): the future of data protection by design and default', *International Data Privacy Law*, 2020, pp. 40 et seq.

295 See also European Data Protection Board, *Guidelines 4/2019 on Article 25 – Data Protection by Design and by Default,* Version 2.0, p. 29.

296 Proposal for a Data Act, Explanatory Memorandum, p. 14.

297 In this direction Kerber, W., *Governance of IoT Data: Why the EU Data Act will not fulfill its objectives*, p. 8.

related service serves as a general principle applying also in case data is shared with third-parties (see Article 5 (1)). Granting *free* access to the user is justified in the proposal with the 'co-generated' character of the data, in the sense, that the user has 'contributed' to create the data by its use[298] and should therefore be able to 'derive benefit' from it (see Recital 18).

The data holder has to establish a simple request mechanism through electronic means – where technically feasible. Specifying *how* data access should be realised is, compared to the vaguely formulated data portability right of Article 20 GDPR, a real step forward. In practice, the concrete technical and organisational implementation will be the decisive factor (on the provisions for enhancing interoperability, see below 4.7). As described in Recital 20, it might be a workable solution for making the requested data available to the user to rely on user accounts which regularly have to be created for the use of an IoT product. This holds true in particular where several persons use a product.

If the user requests access to data, the data holder should solely request information necessary to verify the 'quality as a user' and must not keep respective information beyond what is necessary for fulfilling the user's request for data access comprehensively, see Article 4 (2). By imposing rather low requirements for the identification of the requesting user on the data holder, the provision seems to aim at making the access mechanism practicable. From a liability perspective, it might however not be 'that easy': The data holder should in any case implement measures for verifying the identity of the user in order to prevent data access by non-authorised parties and also a breach of its contractual obligations (on this issue see below 4.2.5). Also in this regard employing user accounts or a comparable solution can be an effective solution, since the user itself is responsible to prevent misuse of its account.

b. Trade secrets, Article 4 (3)

According to Article 4 (3), trade secrets shall only be disclosed (to the user) provided that all specific necessary measures are taken to preserve the confidentiality of the trade secret, in particular with respect to third parties. Data holder and user can furthermore agree on measures to preserve the confidentiality of the shared data.

i. Co-generated data and trade secrets protection

Data generated by the use of a product or related service can in principle constitute a 'trade secret', as the definition of Article 2 (1) Trade Secrets Directive is construed broadly. According to this provision, information qualifies as trade secret if it is secret (a), has a commercial value because it is secret (b), and is subject to reasonable steps to keep it secret (c).

Data generated by the use of a product or related service (*volunteered* and *observed* data) will regularly be combined, structured and aggregated by the data holder resulting in a large dataset. Such datasets undoubtedly can be trade secrets under the Trade Secrets Directive's definition. By contrast, Article 4 grants access to data generated by one user of an IoT product. But even such individual datasets will often be combined and structured in the collection and observation process

[298] See Proposal for a Data Act, Recital 6; see further *ALI-ELI Principles for a Data Economy – Data Transactions and Data Rights*, Principle 3 (1) (h), see also illustrations at p. 34.

in a particular way and will thus not be generally known in their precise configuration and assembly of their components within the circles that normally deal with the kind of information in question. Also, even one user can undoubtedly generate a substantial amount of different complex datasets in many cases. Therefore, even individual-level datasets, consisting of comprehensive use data from one user of an IoT device will often have to be regarded as secret according to Article 2 (1) (a) Trade Secrets Directive. Further, typically, such information will be subject to reasonable steps for preserving its secrecy (in particular as this condition of protection should not be interpreted too strictly[299]), Article 2 (1) (c) Trade Secrets Directive. As to the requirement of a *commercial value* because of the *secrecy* of the information (Article 2 (1) (b) Trade Secrets Directive), in the case of data (co-)generated by the use of a product, it has been argued that the causal link between secrecy and commercial value existed only for data which give insights into the functioning of the individual device because solely the access of competitors to such information would destroy the data holder's competitive advantage.[300] However, Recital 14 of the Trade Secrets Directive expresses a rather broad understanding of 'commercial value': Even *potential* commercial value suffices and a wide range of interests of the trade secret holder can be taken into account when assessing 'harm' for the data holder. Thus, the definition of commercial value is not restricted to a limited perspective, focusing on direct impact on competitive advantages.[301] In sum, individual-level datasets resulting from the use of IoT products and the related collection of volunteered and observed data can be protected as trade secrets under the definition of Article 2 Trade Secrets Directive. Given the large variety of products, related services, use scenarios and data covered by the Data Act, the character of the affected datasets as trade secrets can only be assessed on a case-by-case basis, but, undoubtedly, the obligations under Article 4 and 5 will regularly apply to trade secret protected datasets.

ii. Acquisition and use of trade secrets

Where trade secrets protection is affected, Article 4 (3) attempts to strike the necessary balance by requiring that trade secrets shall only be disclosed provided that all specific necessary measures are taken to *preserve their confidentiality* in particular with respect to third parties. In regard to *limited disclosure of and access to* the information, this does indeed appropriately address the problem that such access should by no means lead to the datasets losing their character of a trade secrets because of losing their secrecy. At the same time, if the respective conditions are met, Article 4 (3) Data Act legitimises the acquisition of the trade secrets by the users of the products, so that their *acquisition of the trade secret* is not unlawful and thus not actionable under Article 4 (1) Trade Secrets Directive.

In fact, in the context of the Trade Secrets Directive this lawful acquisition also legitimises *subsequent acts of use* and *certain acts of disclosure* to third parties. This is because under Article 4 (3) Trade Secrets Directive, use or disclosure of a trade secret is only regarded as unlawful, if the trade secret was acquired unlawfully (which because of Article 4 Data Act is not the case), if disclosure was in breach of a confidentiality agreement or any other duty not to disclose the trade secret (here Article 4 (3) Data Act comes into play which requires all specific necessary measures to be taken to preserve confidentiality), or if subsequent use was in breach of a contractual or any other duty to limit such

[299] This follows from the objective of trade secrets protection to reduce transaction costs for factual protection measures, see Lemley, M., 'The Surprising Virtues of Treating Trade Secrets as IP Rights', *Stanford Law Review*, 2008, p. 348 et seq.

[300] See e.g. Drexl, J., *Data Access and Control in the Era of Connected Devices*, p. 94.

[301] See also Aplin, T., 'Trading Data in the Digital Economy: Trade Secrets Perspective', pp. 65 et seq.

use (here Article 4 (4) Data Act comes into play which prohibits use of the obtained data to develop a product that competes with the product from which the data originate, cf. further c.).

The complex interplay of Article 4 Data Act and Article 4 Trade Secrets Directive thus indeed leads to a consistent result in regard to subsequent use and disclosure acts as follows: Subsequent use and limited disclosure to third parties is legitimate under the Trade Secrets Directive, if all specific measures are taken to preserve the confidentiality of the trade secrets, in particular with respect to third parties (as they can be specified in an agreement between the data holder and the user), and, if such use is not directed at developing a product that competes with the product from which the data originate. If these qualifications are met, subsequent use acts and limited acts of disclosure are not unlawful under Article 4 Trade Secrets Directive. If the user fails to comply with these obligations or any other obligations which were laid down in an additional agreement according to Article 4 (3) Data Act, such use or disclosure will be regarded as unlawful under Article 4 (3) Trade Secrets Directive and thus constitute an actionable infringement under the Trade Secrets Directive (with additional protection against third parties, if they knew or ought to have known about the unlawful acts of the user).

c. No use of data for developing a competing product, Article 4 (4)

Article 4 (4) reflects political caution insofar as it effectively limits the immediate effect of the Commission's proposal to an opening of *secondary* markets (*aftermarkets*) by facilitating access to data generated by IoT products, while excluding any use of such data for the development of products in competition with the product from which the data originate. This indeed is in line with the objective of the Data Act as it is laid down in Recital 28.[302]

According to Article 4 (4), 'the user shall not use the data obtained (…) to develop a product that competes with the product from which the data originate'. In light of the aforementioned (limited) objective, this provision on principle is consequent. However, the scope and the conditions set out in Article 4 (4) are too vaguely formulated and therefore have the negative potential to cause significant chilling effects in regard to the actual use of the acquired data, instead of establishing legal certainty and trust, thus practically fostering the emergence and development of aftermarkets.[303]

First of all, the definition of the relevant market remains unclear despite of being the core condition for assessing whether the products would compete with each other. Although for defining the relevant market of the product from which the data originate, the established standards of general competition law (i.e. demand-side oriented market concept, SSNIP test) naturally come to mind, it should nonetheless be expressly specified (e.g. in the Recitals) what standard of assessment should apply. Secondly, in this context it should also be clarified, whether use for the development of a service or a virtual assistant, related to the product, and thus in competition with respective product elements or services of the data holder is permitted or not; the current wording might seem to allow such use, but since related services (and virtual assistants as part of that concept) have to be an

[302] See Proposal for a Data Act, Recital 28: 'The aim of this Regulation should accordingly be understood as to foster the development of new, innovative products or related services, stimulate innovation on aftermarkets, but also stimulate the development of entirely novel services making use of the data, including based on data from a variety of products or related services'.

[303] Namely, the question of the burden of proof for establishing that certain uses are aimed at developing a product that competes with the product from which the data originate, should also be expressly clarified at least in the Recitals.

inseparable element of the IoT product in question, it is doubtful, whether Article 4 (4) would at least permit to develop related services or virtual assistants which are in competition with respective elements of the original IoT product collecting the underlying data.

Thirdly, in general competition law the possibility of identifying a hypothetical separate upstream market, e.g. a *hypothetical* upstream (licensing) market for essential data or IP, suffices for granting a compulsory licence under Article 102 TFEU, even if the resulting new or improved product or service is in direct competition with products or services of the data or IP holder (if the rather strict general conditions of abuse of a dominant position by denying a licence are met, see above 3.1.5). In addition, prohibiting the use of the obtained data for developing a competing product (in particular also in Article 5) seems to exclude any significant indirect positive effects of the new provisions in the third case group of justifiable data access (e.g. by cumulating large numbers of acquired individual-level datasets in order to develop a new or better product for the primary market). In the context of the 'data package' hitherto solely Article 6 (j) Digital Markets Act proposes a very specific access right for third-party search engine providers which might be in direct competition with gatekeeper search engines; obviously, this might leave gaps in improving data access beyond the practically rather ineffective and difficult to enforce possibilities under Article 102 TFEU (which of course remain applicable if their conditions are met). As for the Data Act with its mixture of broad horizontal applicability throughout the entire IoT sector, complemented with a very limited object and aim of the regulation (only volunteered and observed data, only to foster competition in certain aftermarkets), the limitation in regard to uses in order to develop competing products has certain consistency, as it helps to proportionally mitigate the impact of the proposal on contractual freedom and dynamic competition in regard to the very development of data-generating IoT products.

Nonetheless, the provision in its current wording does not allow to draw a *clear* line in cases in which, for instance, the data holder itself offers (or is about to offer) a complementary product or service and in regard to related products or services (including virtual assistants).[304] In that wider context, it has also to be remarked, that the proposal solely refers to aftermarket *services*,[305] and does nowhere expressly address the question of aftermarket *products*. In sum, Article 4 (4) has to be clarified and further specified (including the question of burden of proof). Besides, it should also be re-evaluated, whether the general prohibition to use the data for developing a competing product can lead to the desired results;[306] in particular, this should certainly be only a non-mandatory default, so that the parties should be able to agree otherwise.

d. Relation to the GDPR, Article 4 (5)

In principle, the provisions on access, use and sharing of data generated by IoT products are designed to cover both, personal and non-personal data. Nevertheless, the requirements for the lawful processing of personal data set forth in the GDPR also have to be fulfilled. This is of particular importance where the user is not the data subject (such as in the case of affected employees, executives etc.). As expressly clarified by Article 4 (5), the transfer of the product-generated *personal*

[304] See also Graef, I. and Husovec, M., *Seven Things to Improve in the Data Act*, p. 2.

[305] Proposal for a Data Act, Recitals 6, 28 and Explanatory Memorandum, pp. 13, 15.

[306] Kerber, W., *Governance of IoT Data: Why the EU Data Act will not fulfill its objectives*, p. 13 et seq.

data to another person/entity than the affected data subjects requires a specific legal basis in the sense of Article 6 GDPR or – for special categories of personal data – Article 9 GDPR[307].

First of all, the data subject's *consent* according to Article 6 (1) (a) GDPR or Article 9 (2) (a) GDPR (requiring *explicit* consent), given for this specific purpose, may serve as a legal basis for making data available to the user pursuant to Article 4 (1) Data Act. *Data holder* and *user* as data recipient (and not being the data subject) will regularly qualify as joint controllers in the sense of Article 26 GDPR, since it suffices that one controller makes it possible for the other to obtain personal data.[308] From a data protection perspective, constellations in which the *user* enables the *data holder* to obtain personal data generated by an IoT product are comparable to the case in which a website operator embeds a social plug-in allowing a social network provider to obtain personal data generated through the website.[309] As a result of the joint controllership of data holder and user, according to Article 26 GDPR they will be obliged to conclude an arrangement in order to allocate the respective obligations and responsibilities transparently.[310] Obtaining the *data subject's* consent (and fulfilling the information duties of Articles 13 and 14 GDPR) would – again comparable to the social plug-constellation – fall within the *user's* responsibility and would be required before a collection of the data affected subjects' personal data by the IoT product begins.[311] However, often the strict conditions for valid consent, the relatively static character of the concept (in particular with regard to dynamically changing agents and purposes of data processing), as well as the possibility to withdraw the consent anytime, make acquiring valid and resilient consent a rather cumbersome, cost-intensive and unreliable route towards compliance with the GDPR.[312]

Making data available to the user on basis of Article 6 (1) (b) GDPR will regularly not be possible as this would require a 'contract to which the data subject is party', thus, a contractual relationship between data subject and data holder.

To be sure, according to Article 6 (1) (f) GDPR making data available to the user may often qualify as pursuing a legitimate interest of either the *user* (enforcing its access right according to Article 4 (1)) or of the *data holder* (complying with its obligation to make data available according to Article 4 (1)) as far as these interests are not overridden by the interests or fundamental rights and freedoms of the data subject. From the perspective of the involved businesses and in regard to the objective of the Data Act to effectively foster the emergence and development of data-driven markets, however, the legal uncertainty of relying on the head of Article 6 (1) (f) GDPR will often be a significant hurdle for effective data access and use.

As Article 4 (5) explicitly refers to the GDPR as necessary legal basis for making personal data available to the user. This seems to rule out Article 6 (1) (c) GDPR which could normally 'import' other provisions of Union law, e.g. a provision which obliges the data holder to grant access to certain IoT

---

[307] For particular relevance in the context of virtual assistants with voice-control function: A human voice amounts to 'biometric data', so that the stricter requirements of Article 9 GDPR apply, see European Data Protection Board, *Guidelines 02/2021 on virtual voice assistants,* Version 2.0, paragraph 31.

[308] See CJEU, judgment of 29 July 2019, *Fashion ID v Verbraucherzentrale NRW*, C-40/17, EU:C:2019:629, paragraph 75.

[309] These were the circumstances of the Fashion ID decision: CJEU, judgment of 29 July 2019, *Fashion ID v Verbraucherzentrale NRW*, C-40/17, EU:C:2019:629.

[310] Joint controllership 'does not necessarily imply equal responsibility', rather 'operators may be involved at different stages of that processing of personal data and to different degrees, with the result that the level of liability of each of them must be assessed with regard to all the relevant circumstances of the particular case', see CJEU, judgment of 29 July 2019, *Fashion ID v Verbraucherzentrale NRW*, C-40/17, EU:C:2019:629, paragraph 70.

[311] Cf. CJEU, judgment of 29 July 2019, *Fashion ID v Verbraucherzentrale NRW*, C-40/17, EU:C:2019:629, paragraph 102.

[312] Leistner, M., Antoine, L. and Sagstetter, T., *Big Data,* pp. 248 et seq.

data, into the GDPR bases for lawful personal data processing. Otherwise, Article 6 (1) (c) GDPR could effectively pave the way for genuinely reducing the impact of and the difficult distinction between personal and non-personal IoT data, if Article 4 (1) and Article 5 (1) were recognised as legitimate 'legal obligation' in the sense of Article 6 (1) (c) GDPR. As the *user* will qualify in many cases as (joint) controller, he/she would still be obliged to fulfil all requirements set forth in the GDPR and would also be the responsible addressee for enforcing the data subject's individual rights. As a result, the data subject's rights would not be affected negatively in this case.

In practice, the involvement of personal data, which often is merely incidental (at times manifestly public) and which might also be an issue where at first sight only business data are used (e.g. in the case of smaller companies as users, where owners, partners, a limited number of stakeholders or employees might be identifiable), is a *major obstacle* to the efficient development of valuable contextualised datasets and data-driven markets. It is therefore recommended, that in order to make the newly proposed provisions work effectively in practice, Article 4 (1) and 5 (1), could be regarded as relevant obligations of Union law, to which the data holder is subject, and which should thus be a *legitimate base for lawful data processing according to Article 6 (1) (c) GDPR*. Recital 24 could therefore express that any processing of personal data requires a legal basis pursuant to the GDPR, and clarify that the obligations set forth in the Data Act can qualify as 'legal obligation' in the sense of Article 6 (1) (c) GDPR. In the systematic context of the Data Act and the GDPR this would indeed lead to an overall consistent result: For general personal data, Article 4 (1) and 5 (1) would effectively be regarded as a legitimate basis for lawful processing of such data, while the concept of (joint) controllership would ensure that the rights and interests of the concerned data subjects would nonetheless be safeguarded in regard to subsequent processing by the user. For sensitive data, the conditions of Article 9 GDPR would inevitably apply, thus leading to stricter conditions, unless the concerned personal data were manifestly made public by the data subject (see Article 9 (2) (e) GDPR).

In sum, compared to the current status quo, the Data Act does not impose additional 'hurdles' for the processing of personal data generated by the use of an IoT product. However, the Data Act does not contribute to reducing complexity or legal uncertainty in regard to the processing of personal data either. The implementation of the access and use rights proposed by the Data Act is based on a complex network of (bilateral) contractual agreements (see further, immediately below). In addition, when personal data are concerned (which because of the broad definition of personal data will often be the case even if the concerned individual-level datasets on their face seem to be anonymised non-personal data), requirements, such as joint controllership agreements, according to Article 26 GDPR etc., must be considered. While this is perfectly in line with the GDPR's concept and structure, the unmitigated cumulative combination of the GDPR's structures and requirements with further regulatory intervention adds new layers of complexity, of particularly necessary personal data related agreements, of personal data-related requirements, information duties, shared responsibilities, resulting liability risks etc. Large parts of the data generated by an IoT product will qualify as personal data (even if this does not seem to be the case for a diligent operator without specific legal knowledge of data protection law) as long as the definition is not refined in a way that allows to clearly distinguish between personal and non-personal data with sufficient legal certainty. Even more problematic, data generated by IoT products that record health data, voice etc. will be subject to the stricter requirements of Article 9 GDPR as special categories of data.[313] In fact,

[313] With respect to Article 9 GDPR it should be noted that in 2021 the Austrian Supreme Court (OGH) has referred a question concerning the definition of special categories of personal data in the sense of Article 9 (1) GDPR to the CJEU

these are practical problems that have to be solved for making a data-driven economy work in the Union. That does not mean to limit the data subjects' rights and protection, but it does mean that they have to be delineated properly. Thus, in a short-term perspective, our proposal with regard to Article 4 (1) and Article 5 (1) as legitimate bases for lawful data processing under Article 6 (1) (c) GDPR might be helpful (though properly difficult to agree upon politically). In the long run, reliable standards for anonymisation of data, which relieve businesses, which have complied with these anonymisation standards in regard to certain datasets, in a reliable and future-proof way from the requirements of the GDPR for those datasets (even if de-anonymisation is possible for certain third parties or at a later point in time), seem necessary and should be considered.

e. Use of non-personal data based on contractual agreement, Article 4 (6)

Article 4 (6) constitutes a crucial change in comparison to the current status of non-personal data and could be seen as a real (although somewhat hidden and hopefully sufficiently flexible) paradigm shift. This is because – at worst – the provision could result in a significant degree of factual allocation of control over the use of non-personal data generated by an IoT product or related services to the user alone.

According to Article 4 (6) '[t]he data holder shall only use any non-personal data generated by the use of a product or related service on the basis of a contractual agreement with the user'. Hence, the user has to 'authorise' use of non-personal data collected by an IoT product by means of a contract.[314] This implies that contractual control over the use of respective non-personal data is assigned to the user although neither the fundamental rights protecting personal data nor an exclusive IP or other property right apply. On the contrary, under the Database Directive's sui generis right, the CJEU has wisely refused (exclusive) protection for data generated as a spin-off of another main business activity.[315]

While the underlying ratio to empower users in regard to data generated by their very activity undoubtedly holds water for personal data (due to the fundamental rights of the data subjects), from our viewpoint this is not generally warranted for non-personal data.[316] Often, the investments of the manufacturer to observe the data in question will by far exceed any indirectly relevant investments of the user of an IoT product. It is therefore hard to understand the general necessity of Article 4 (6) in the IoT field at all. One might explain the provision as remedying an information problem: The necessary conclusion of a contract might help to inform the user about data-related collection and observation activities and envisaged uses by the IoT provider. However, such provisions would seem more important in the field of data related *services* (cloud services, AI-toolkits and online services etc.), where general fishing for data (in order to use them for own general purposes) seems to be a more imminent problem than throughout the entire IoT sector.

---

for a preliminary ruling pursuant to Article 267 TFEU, see OGH, judgment of 23 June 2021, *Schrems v Facebook Ireland*, 6 Ob 56/21k.

[314] See also Recital 24 Proposal for a Data Act: '(…) the basis for the manufacturer to use non-personal data should be a contractual agreement between the manufacturer and the user'.

[315] CJEU, judgment of 9 November 2004, *British Horseracing Board v Hill*, C-203/02, EU:C:2004:695, paragraphs 30 et seq.

[316] Schweitzer, H. and Peitz, M., 'Ein neuer europäischer Ordnungsrahmen für Datenmärkte?', *Neue juristische Wochenschrift*, 2018, p. 280.

Besides, the question is how effective Article 4 (6) will actually be in achieving its goal, if this goal was remedying an information asymmetry (which we cannot identify across the board in the entire IoT sector) through enhancing transparency in regard to actual or envisaged upstream data uses or transfers. The necessary contract between user and data holder will be governed by *national law*. In this regard, the question arises what should be the *subject* of the contract as no '(exclusive) right' or any other clearly licensable position is concerned – which in certain constellations (although not in normal cases) might even raise competition law concerns. In addition, when concluding a contract for the purchase, rent or lease of a product, an *implied* agreement[317] will often have to be assumed in respect to the use of the non-personal data generated by the respective product (or related services) anyway, although the conditions and detailed scope of such an implied contract element will depend on the respective provisions of national contract law. Therefore, if the provision was meant to enhance *transparency* for the user when acquiring a data-collecting IoT product, this should be expressed clearly and specifically. However, the information duties stated in Article 3 (2) already serve that goal. All in all, Union law should not impose any additional requirements for contractual bases for data use by the data holder, as this would be dysfunctional in regard to the general objective of the Data Act, i.e. to foster the emergence and competitiveness of IoT data-based markets by adding considerable transaction costs to the equation.[318]

Moreover, from our viewpoint an *obligation on the side of the user* to allow such data use *upon request of the data holder*, if it is in line with the principle of good faith and if no legitimate interests of the user are disproportionally harmed, should be added to clarify that the user should not have an unmitigated 'veto right' in that regard (Article 13 (4) (c) already goes into that direction, but should be generalised and broadened). In fact, typically, both parties equally contribute to the collection, observation and configuration of use data which is why a predominant (almost factually exclusive) role of the users in regard to further applications of such data can hardly be justified and would certainly not serve the goal of effectively opening additional data-related markets, as often the data holder will be in a better position to identify, utilise and capitalise market possibilities for its own or third party use of such data. If such an obligation on the side of the user were considered, one should also complement this with practical *procedural rules*; in particular, if informed users did not veto certain upstream uses by the data holder (including transfer of the data) within a given period of time, it should be presumed that they agree with the upstream use in question.

In such an understanding, Article 4 (6) second sentence, i.e. the data holder's obligation not to use the data for deriving 'insights about the economic situation, assets and production methods of or the use by the user that could undermine the commercial position of the user', would be an example for legitimate interests which would justify the user in denying the necessary contractual agreement with the upstream use of its individual use data. The provision limits the possibility of the data holder to deduce information (= inferred data) concerning certain competition parameters essential for the commercial position of the user in its relevant markets. A certain parallel can be drawn here to Article 6 (1) (a) of the proposed Digital Markets Act; however, this provision only applies to gatekeepers. In equal contractual relationships, to be sure, such use of inferred data should give rise to a veto right by the user; however, this should not be a generally mandatory provision, instead the user should still have the possibility to contractually agree with such uses, if he was willing to do so.

---

[317] Recognised also by European soft law principles, e.g. Article 6:102 Principles of European Contract Law (PECL); Article 5.1.2 Unidroit Principles.

[318] Cf. Kerber, W., *Governance of IoT Data: Why the EU Data Act will not fulfill its objectives*, p. 2 et seq., p. 20 et seq.

According to the Data Act, recent developments such as the EU 'Code of Conduct on agricultural data sharing by contractual agreement'[319] should serve as examples or basis for the agreements required by Article 4 (6) (see Recital 25). For the agricultural sector, this Code explicitly allocates the data to the *'data originator'* who 'has created/collected this data either by technical means (e.g. agricultural machinery, electronic data processing programs), by itself or who has commissioned data providers for this purpose'.[320] While therefore the farmer is not necessarily the 'data originator' (e.g. when data is collected automatically by technical means), it remains rather unclear who should qualify as 'originator' if it is not the farmer: the owner, controller or (lawful) user of the machine?[321] The Code seems to rely on the ownership of the sensors which collect the relevant data.[322] The collection, access, storage and usage of such data require the originator's permission by means of contractual consent which should also include, inter alia, for which purposes the data is shared.[323] The Data Act goes one step further by tending to generalise these rules, which were originally only exemplarily proposed for the agricultural sector by means of a voluntary, self-regulatory instrument, in a statute; at the same time it simplifies these rules by allocating the power to give the necessary contractual consent to the users alone without taking into account the complexities and flexibilities set out in the Code. In fact, as the Code of Conduct refers to the 'data originator', it leaves considerably *more flexibility* than the Data Act 'entitling' the 'user'. While in B2C relations, arguably the user should have the possibility to control the data generated by his or her use of an IoT product, at least in B2B relations it should be put under scrutiny whether the 'user' of a product is always the adequate addressee for such a right to consent.[324] From our viewpoint, the reference to the Code rather strengthens our argument, that actually *both* parties to an IoT sale/rental/lease agreement should be at liberty to use the resulting volunteered or observed data, if legitimate interests of the respective other party are not disproportionately harmed by such use. The very nature of *'co-generated'* data[325] and the general concept of reciprocity[326] can serve as additional arguments in this

[319] For an in-depth analysis see Atik, C. and Martens, B., 'Competition Problems and Governance of Non-personal Agricultural Machine Data: Comparing Voluntary Initiatives in the US and EU', *Journal of Intellectual Property, Information Technology and E-Commerce Law*, 2021, pp. 381 et seq.; van der Burg, S., Wiseman, L. and Krkeljas, J., 'Trust in farm data sharing: reflections on the EU code of conduct for agricultural data sharing', *Ethics and Information Technology*, 2021, p. 185 et seq.

[320] See EU Code of conduct on agricultural data sharing by contractual agreement, 2018, p. 6. In the US already 2014 an initiative of the American Farm Bureau Federation was launched leading to 'Core Principles' for Agriculture Technology Providers according to which 'farmers own information generated on their farming operations' (available at: https://www.agdatatransparent.com/principles).

[321] Atik, C. and Martens, B., 'Competition Problems and Governance of Non-personal Agricultural Machine Data: Comparing Voluntary Initiatives in the US and EU', *Journal of Intellectual Property, Information Technology and E-Commerce Law*, 2021, pp. 382 et seq.

[322] EU Code of conduct on agricultural data sharing by contractual agreement, 2018, p. 15.

[323] EU Code of conduct on agricultural data sharing by contractual agreement, 2018, p. 8 et seq. The Code entails a portability right that can however be overridden by contract, p. 9 et seq.

[324] Kerber, W., *Governance of IoT Data: Why the EU Data Act will not fulfill its objectives*, p. 21.

[325] See e.g. the different factors described in *ALI-ELI Principles for a Data Economy – Data Transactions and Data Rights*, Principle 18.

[326] For instance, the Consumer Data Rights in Australia entails a reciprocity clause. See further on this Deloitte and others, *Study to support an Impact Assessment on enhancing the use of data in Europe*, p. 212 et seq. – using this consideration for defining the Study's policy options. In addition, the *ALI-ELI Principles for a Data Economy – Data Transactions and Data Rights*, contain a reciprocity clause, see Principle 27. Furthermore, comparable approaches exist for defining FRAND conditions under general competition law (cf. above 3.3.1.a.vi and further Leistner, M., Antoine, L. and Sagstetter, T., *Big Data,* p. 454 et seq.).

regard. Such more flexible interpretation would further allow to address situations with *multiple actors* adequately, for instance where component suppliers are involved.

f. Main changes through the Data Act

In comparison to the existing (portability) rights of Article 20 GDPR and Article 16 (4) Digital Contents Directive, the main extension for natural persons as users of an IoT product or related service through the Data Act consists in the possibility of access to and use of volunteered and observed *non-personal data* generated by the use of a product at any time, including real-time access.[327] Inferred data, however, is not subject to the access and use rights proposed in the Data Act either.

For business users (B2B relations), the Data Act results in a significant extension of the possibility to access and use data generated by an IoT product or a related service.[328] In contrast to the planned Article 6 (i) Digital Markets Act, access to volunteered and observed data generated by use of products and related services is not only granted in relation to gatekeepers, but in relation to *all* IoT data holders (besides micro and small enterprises).

g. Summary

The access and use right for users of IoT products or related services set forth in Article 4 address the first case group of justifiable access rights, we have outlined, by granting access to *individual-level use data*. As the result of a conscious (albeit sweeping) political decision, the access and use rights (as well as the sharing rights provided for in Article 5) apply equally in B2C as in B2B relations (only micro-sized and small enterprises as IoT producers (data holders)) are exempted. As we have discussed, compared to the services sector, which is not addressed in the Data Act, and where only very large gatekeeper platforms are subject to (comparatively limited) access and portability duties, this constitutes a remarkable burden on IoT producers (in particular on middle-sized enterprises).

Even though the proposal does not intend to award 'exclusive rights of access and use' (see Recital 6), in particular Article 4 (6) leads to a certain degree of factual allocation of contractual *control* over the use of non-personal data (co-)generated by IoT products to the *users* of such products. This becomes even more apparent in the context of Article 5 establishing a right to share data with third parties (see immediately below). However, it seems that in light of the Data Act's objective, i.e. to foster the emergence and competitiveness of certain aftermarkets and related markets, it would be equally important to expressly allow the IoT producers (*data holders*) to use and share non-personal IoT data (as well as personal IoT data to the maximum extent possible under the GDPR), if this is compliant with competition law rules, in line with good faith and if no legitimate interests of the users are disproportionately harmed by such upstream use and sharing.

The relation to trade secrets is satisfyingly addressed in Article 4. By contrast in relation to personal data at least some clarifications and simplifications should be considered, which seem possible without changing the provisions of the GDPR. On the long run, changes or amendments to the GDPR will be needed as well.

---

[327] Both is fundamental precondition e.g. for multi-homing, Metzger, A., 'Access to and porting of data under contract law: Consumer protection rules and market-based principles', p. 292.

[328] In regard to the open questions in regard to the justification of the proposed access and use rights in B2B relations see above 4.2.1.b.

Whereas the prohibition of use to develop a competing product is in principle in line with the Data Act's limited objective to open and to foster secondary and aftermarkets, at least the conditions for defining the term 'competing product' should be further clarified and specified.

4.2.4. Right to share data with third parties (Articles 5 and 6)

Article 5 (1) stipulates the *user's* right to *share* data generated by a product or related service with third-parties. According to the provision's wording, the user has to either request to make the respective data available to a third party or 'authorise' a third party to act on his/her behalf. Article 5 (1) corresponds with the scope of Article 4 as the same data categories and even real-time access are entailed. While sharing the respective data with third parties should be free of charge for the user, the data holder has to be compensated by the third party for making the requested data available (see further below 4.2.5.b).

Hitherto, such sharing or portability rights are only foreseen in regard to personal data and as a mere post-contractual duty in B2C relationships. According to the portability right of Article 20 GDPR, a data subject is entitled 'to have the personal data transmitted directly from one controller to another, where technically feasible'.[329] Article 16 (4) Digital Contents Directive does not foresee a direct data transfer to another provider. Concerning Article 20 GDPR, the standard for determining whether a transmission is technically feasible and particularly, which steps a controller has to take for making a direct transmission possible, is rather unclear. Article 5 tackles this problem as the technical feasibility of third-party access has to be guaranteed by the data holder (see Recital 31).

a. Requirements for third party access: request or authorisation by the user

Article 5 (1) requires a request by the user for triggering the sharing of data with third parties, i.e. to make data available to a third party; the request can also be made by a party acting on behalf of the user. Third parties are obliged not to coerce, deceive or manipulate the user in order to get access by means of the sharing right pursuant to Article 5 (see Article 6). Neither shall they deploy coercive means or abuse evident gaps in the technical infrastructure of the data holder in order to obtain access to the data (see Article 5 (4)).

In particular, the possibility for third parties to act on behalf of the user seems to be an important implementation tool for facilitating access for third parties in constellations governed by Article 5. Such agency solutions will certainly be necessary if the newly proposed tools shall work effectively in practice at all. In addition, this construction should also serve as 'blueprint' for allowing transfer or fiduciary exercise of portability/access rights in order to enforce them more effectively (see on this aspect further below).

Where the user authorises a third party to act on his/her behalf, it might be clarified further how this could be easily proven in practice. In general, practical problems comparable to those for obtaining a data subject's consent for the processing of personal data in the context of multipolar settings could arise. In order to contribute to an effective and workable mechanism for facilitating data

[329] See for instance, Polański, P., 'Some thoughts on data portability in the aftermath of the Cambridge Analytica scandal', *Journal of European Consumer and Market Law*, 2018, p. 142.

sharing on basis of Article 5, technical solutions and interfaces will have to be developed.[330] In this context interoperability and interconnectivity will again play a key role as the different actors have to 'cooperate' at the very least in a contractual tri-angle (but probably more often in entire networks of such tri-angles). As comparably discussed for personal data, the need for requests to share and use non-personal data (generated by the use of an IoT product) might be implemented by data storage or 'consent' management systems run by data intermediaries or particular platform services. Whether such business models will evolve, remains to be seen and will very much depend on the question whether there are sufficient *incentives for users* to initiate data sharing on a broader scale (which the Commission assumes in its Data Strategy[331]).

The Data Act generally takes up various aspects discussed for personal data and applies them to non-personal data. This also concerns the idea of a *rather granular, specific* '*consent*' or *request* by the user and the option to withdraw permission (cf. Recital 25). If one followed this approach with its full consequences, indeed some of the difficult problems of distinguishing personal and non-personal data would be 'resolved'. However, it would then be necessary to align the requirements of the GDPR in order to reduce legal uncertainty. Also, the transplant of personal data related concepts, such as rather granular, comparatively static structures for consent (and in particular the right to withdraw consent), to non-personal data comes with a significant price-tag. From our perspective, a correspondingly granular allocation of control (including options to withdraw permission) over the use of *non-personal* co-generated data to the user cannot be justified as this would make the practical implementation of the newly proposed provisions as well as data collection and sharing by data holders disproportionately cumbersome and costly in B2B settings. Thus, the immensely high requirements for personal data should certainly not serve as respective standard for non-personal data. In the context of non-personal data in B2B relationships, undoubtedly, broadly formulated and binding umbrella consent, broad and binding sharing requests, agency solutions as well as free transfer and fiduciary exercise of portability/access rights of the business users should be possible in IoT markets. Even with all these instruments and possibilities in place (as they are currently not in Article 6), it seems by no means certain that users will have sufficient incentives to request data sharing from their IoT providers.[332]

For this reason and corresponding to our general criticism of allocating non-personal data access and sharing rights 'proto-exclusively' to the users, moreover, we would propose to verify whether the *user* alone should be given the decisive role for facilitating data sharing with third-party as far as *non-personal* data are at stake or when the respective conditions under the GDPR are met anyway. This is because there might be situations, where the *data holder* is in a much better position to make use data available to third parties and in such situations, the data holder should undoubtedly remain free to do so, if this is in line with competition law, the principle of good faith and does not disproportionately harm legitimate interests of the users (see also above 4.2.3.e). To be sure, the current proposal could (and should) be read in a way that only a *right* to initiate data sharing is allocated to the users, while on principle the *liberty* of the data holders to share data should remain unscathed. However, Article 4 (6) and several Recitals of the Data Act (i.e. 31, 33 et seq.) suggest that any act of upstream sharing by the data holder would at least have to be subject to contractual

[330] In that regard the issue of mere in situ access vs. genuine data transfer claims should also be further considered. In situ access can have certain advantages (e.g. personal data protection issues can be less imminent depending on the technical circumstances), but literature has already pointed out that it might be insufficient in certain sectors (see Kerber, W., *Governance of IoT Data: Why the EU Data Act will not fulfill its objectives*, p. 8 et seq.).

[331] European Commission, *A European strategy for data*, COM/2020/66 final, 2020, p. 10.

[332] Only in regard to trade secrets, stricter limitations might be necessary to sustain a workable level of control over such trade secrets of the original user or the data holder down the chain of third-party use (see 4.2.4.d).

consent by the affected user(s), effectively allocating a rather central role for the working of the entire proposed mechanism to the users. While this might be workable in practice if such user consent can be expressed in broad and flexible umbrella contractual clauses as well as by way of implied consent etc., as long as the requirements of the principle of good faith are met, it would add considerable additional transaction cost, if stricter structures or requirements for such users' consent would be applied or considered either under the current structures of the proposed Data Act or under Member States' laws in the future. Therefore, it is suggested to clarify, that the new use and sharing rights of IoT users should not interfere with the principle of contractual freedom (in particular in B2B settings), according to which the data holders can be broadly and flexibly authorised by the users to use and share co-generated data in upstream markets on their own initiative. Moreover, it should be laid down that the users must not deny consent to such sharing activities of the data holders if such upstream use and sharing is in line with the principle of good faith and does not disproportionately harm legitimate users' interests (thus, effectively generalising and broadening Article 13 (4) (c)).

To give just one example of the practical limitations following from the current, comparatively purpose-bound concept of third-party use: As explicitly stated by Recital 33, the third party receiving the data as requested by the user, may solely use the data for the purposes *agreed* with the user. The third party itself may share the data with another third party only if this is necessary to provide the service requested by the user. Consequently, according to Article 6 (1) the *third party* and the *user* have to agree on the purposes and the conditions of making data available to another third party pursuant to Article 5. Additionally, Article 6 (2) implements further obligations of the third party concerning the relation between user and third party. As a result of these obligations for third parties, the Data Act seems primarily designed to enable effective data access and use by third parties in but one central use scenario: The owner of a connected device which he/she bought from the manufacturer (being the data holder in this case), wants to get the device repaired or otherwise serviced or supplied by a third party (including e.g. insuring the use of the device). Thus, the 'user' agrees with the third party on the delivery of respective services and, in addition, authorises the third party to access and use the data collected by the device's use for this particular purpose. Whereas this is undoubtedly an important constellation in which to foster secondary markets (e.g. for repair and other secondary services etc.), it can certainly not provide a basis for facilitating large-scale data sharing. If the Data Act aims at enhancing data sharing beyond this specific use scenario, it has to be reviewed whether and how the highly complex network of different *bilateral* agreements between the different parties could be 'untangled' and framed in a less complicated and more practicable way.

b. Protection of third parties, Article 5 (5)

Article 5 (5) concerns the relation between data holder and third party: According to this provision the data holder shall not use the data generated by the product to gain insights about the economic situation and further business information of the third party, unless the third party has consented. Recital 29 specifies in this regard that 'the data holder should not abuse its position to seek a competitive advantage in markets where the data holder and third party may be in direct competition'.

c. Relation to GDPR, Article 5 (6)

Along the lines of Article 4 (5), Article 5 (6) states that making personal data available to a third party requires a legal basis pursuant to Article 6 GDPR (or Article 9 GDPR as far as special categories of personal data are concerned) if the user is not the data subject. In this regard, the considerations discussed above (see 4.2.3.d) apply equally. In this case, if our proposal above to justify such uses under Article 6 (1) (c) GDPR were not followed and where the conditions of Article 6 (1) (f) GDPR are not certainly enough met, the *user* would be responsible for obtaining the data subjects' *consent* for making personal data generated by the use of a product available to a third party. In this context, it seems particularly difficult to fulfil the requirement of a 'specific' consent, as the precise third parties (down the line) that should be authorised by the user to obtain data, will not and cannot always be known in advance if the Data Act's sharing provisions shall work effectively in practice. The Data Act does not address the question whether the third party joins as an additional joint controller which would require a joint controllership agreement according to Article 26 GDPR. On the one hand, the data holder factually enables the third party to obtain the respective personal data, so that they could qualify as joint controllers. Article 5 (7) GDPR might be interpreted in this direction as it indirectly refers to an agreement between data holder and third party for the *transmission* of data. However, as the user has to determine the purposes of the *use* of the transmitted data in relation to the receiving third party, it would be more convincing to assume an (additional) joint controllership between user and third party. At the end of the day, user, data holder and third parties are in any case 'controllers' and do therefore have to fulfil the GDPR's requirements (cf. Article 6 (1) Data Act).

From our viewpoint, ideally both Article 6 (1) (c) and (f) GDPR, could therefore serve as legal bases as already discussed above (4.2.3.d), and in particular, also a legitimate interest of the *third party* (e.g. fulfilling the purposes agreed with the *user*) can suffice in regard to Article 6 (1) (f) GDPR.

In the wider context of the relationship to the GDPR, finally, Article 6 (2) (b) raises the question whether the addressed 'profiling' is meant to be allowed by the provision as far as it is necessary to provide the service requested by the user and without fulfilling the additional requirements of the GDPR. However, due to the general conception of the Data Act, the provision rather seems to have mere clarifying character with respect to the limitation of the third party to generally act within the limits of the *purposes* for the use agreed with the user, instead of establishing a new 'legal basis' for profiling outside the GDPR.

d. Trade secrets, Article 5 (8)

Compared to the user's access right set forth in Article 4 (3), third-party access to trade secrets underlies additional requirements laid down in Article 5 (8): First, *user* and *third party* generally have to conclude a contract determining the purpose for which the data is made available (cf. Article 6 (1)). Second, the disclosure of the trade secret has to be strictly necessary for fulfilling this purpose. Third, *data holder* and *third party* have to agree on necessary specific measures for preserving the confidentiality of the information which have to be implemented by the third party. This agreement shall further specify the data's nature as trade secret.

In the context of Article 4 Trade Secrets Directive, such agreements will naturally also have to specify necessary limits on the *use* of the trade secret by the relevant third parties. In that regard it is suggested that it should be clarified that such (direct or indirect) *uses* should as well be strictly limited to what is necessary to fulfil the purpose for which the data is made available, unless the parties agree otherwise. In such cases, a definition of specific uses is indeed inevitable in order not to unjustifiably interfere with trade secrets protection. Under the Trade Secrets Directive, such

limitations would then even bind further (other) third party users on the condition that they knew or ought to have known, under the circumstances, that the original third party was acting in breach of contractual duties when disclosing or using the information.

e. No use of data for developing a competing product, Article 6 (2) (e)

Along the lines of Article 4 (4), third-parties receiving data upon request of the user may not use this data for developing a product competing with the data-collecting product or share the data with another third party for that purpose. The concerns we have outlined above (see 4.2.3.c), apply even more urgently in the context of Article 6 (2) since third-party recipients will regularly be active on the relevant markets, e.g. by providing repair or other aftermarket services (cf. Recital 29) where different delineation issues might arise, e.g. in relation to related services provided by the data holder.

The additional obligations laid down in Article 6 for third parties receiving data as a result of Article 5 (1) correspond with the general framework set out by the provisions of Chapter II and will be addressed, where directly relevant, in the following.

f. Summary

The right to share data with third parties as provided for by Article 5 amounts to a 'continuation' of the *user's* right to access and use data generated by an IoT product or related service (Article 4). In principle, it is therefore consequent to rely on a 'user-centric' design of Article 5. However, the concept of expressly enabling only the user to initiate sharing of co-generated data with third parties seems to be primarily tailored to the situation in which the user requests a specific aftermarket service provided by a third party and the respective data should be made available to the latter for this particular purpose. This is in line with the Data Act's general objective to foster the development of aftermarkets in the IoT sector by minimising de facto control over data and establishing a legal framework for respective data flows. However, as a result of the far-reaching allocation of sharing rights in regard of co-generated non-personal data to the users, the provision can lead to a highly complex network of necessary bilateral contracts, further complicated by the additional requirements of data protection law. Particularly because the users have to authorise any third-party access to non-personal data, at the end of the day, the practical difficulties existing in regard to obtaining consent for the processing of personal data in multipolar settings could arise in a comparable form. From our viewpoint, any possibility to flexibilise this system (broad umbrella-requests; third parties acting on behalf of the user including agency, transfer of and fiduciary exercise of sharing rights) should be used (at least when trade secrets are not concerned). Also, the sharing obligation under the conditions of Article 5 should be regarded as a legal basis for processing of personal data under Article 6 (1) (c) GDPR.

The Data Act intends to address the second case group of data access (for competitors in order to establishing competition at secondary markets) for the particular 'sector' of data-generating products. Due to its construction, Article 5 facilitates primarily *occasional* and *selective* data sharing but is not suitable to foster *large-scale* data sharing. The third party has to 'collect' every dataset individually by means of a contractual agreement with the user resulting in high transaction and

information costs.[333] The current design of Article 5 is not necessarily a weak point of the proposal, but it has to be highlighted that it is mainly tailored to fit but one *particular scenario*.

If the legislator wanted to broaden this approach, in addition, it should be expressly clarified that the data holder should also be in a position to share IoT use data on the basis of respective contracts (including on the basis of broad umbrella terms, implied consent etc.), where this is in good faith vis-à-vis the affected users and if it does not disproportionately harm their respective interests. Under these circumstances, an obligation of the users to consent to upstream sharing under the said conditions, should be considered.

With respect to the Data Act's aim to effectively open secondary and aftermarkets in the IoT sector, the prohibition of the use of co-generated data for developing competing products should be clarified and specified in its extent (in particular in regard to related services including virtual assistants).

The difficult relation to the GDPR remains an overall problematic issue. We have made practical proposals on how to effectively achieve the objectives of the proposed Data Act while preserving a high level of protection of personal data and without a need to change the wording of the GDPR.

4.2.5. Obligations for data holders obliged to make data available (Chapter III)

Articles 8–12 determine obligations for data holders obliged to make data generated by an IoT product available to a third party under Article 5 (see Article 12 (1)). In the context of these provisions, the third party is referred to as the 'data recipient'. Articles 8 and 9 establish the FRAND principle in regard to contract terms and compensation. Article 10 proposes a dispute settlement mechanism and Articles 11 and 12 specify the data recipient's obligations.

a. FRAND terms for making data available (Article 8)

According to Article 8, the data holder and the data recipient have to *agree* on FRAND terms and a respective compensation (on this, Article 9) for making the data available as requested by the user. Thus, if the user 'authorises' a third party to access and use the data generated by his/her use of an IoT product, the conditions still have to be settled between data holder and third party. Any contractual term that deviates from the access and use rights set forth in Chapter II is (according to Article 8 (2)) void, hence, these provisions are mandatory in nature – even for B2B relations. From our viewpoint – for the sake of clarity and legal certainty – it should be clarified that such FRAND 'licences' will also cover necessary and justified use acts in regard to trade secrets. This would be of mainly clarifying character as the necessary justification already follows from Article 4 (3) and Article 5 (8) (see above 4.2.3.b.ii). However, it would also allow to take the character of certain data as trade secrets into account when further specifying the terms and range of FRAND compensation.

i. Exclusive agreements, Article 8 (4)

Pursuant to Article 8 (4), the data holder should not make data available to data recipients on an exclusive basis – unless requested by the user. Avoiding exclusionary access is coherent with the

[333] See already Schweitzer, H., 'Datenzugang in der Datenökonomie: Eckpfeiler einer neuen Informationsordnung', *Gewerblicher Rechtsschutz und Urheberrecht*, 2019, p. 575.

Data Act's objective to prevent the development of data-dominating 'gatekeepers' in the IoT sector. It seems questionable, however, whether the *user* should be enabled to request an exclusive agreement as due to Articles 8 and 9 it is explicitly left to the *data holder and the data recipient* to agree on the specific conditions for making data available. As the framework proposed with the Data Act assigns the control over initiating the sharing of data generated by the use of a product to its user, it is a consistent consequence that the user can decide whether to assign an exclusive use right to the data recipient. However, in regard to the goal of opening and fostering competition in secondary markets, this central (and in that regard exclusive) position of the user seems to be contra-productive. From a market-oriented perspective, in constellations in which the respective data is *not indispensable* for operating at a secondary market, granting exclusive access might be justified, for instance, at least for a particular period of time, e.g. for establishing a new service. However, this should also be possible for the data holder in situations outside Chapter II of the Data Act in certain situations and in particular, the equal right of the data holder to share co-generated data should not be hampered by the users' legal position under Article 8 (4). Therefore, we propose that the user should only be enabled to request the making available of data on an exclusive basis, if the respective request is in line with the general principle of good faith and does not disproportionately harm legitimate interests of the data holder.

ii. Relation to trade secrets protection, Article 8 (6)

Article 8 (6) – in addition to Article 4 (3) (concerning the relation between data holder and user) and Article 5 (8) (concerning the relation between the data holder and a third party, designated by the user) – addresses the treatment of trade secrets. This provision reads:

'Unless otherwise provided for by Union law, including in Article 6, or by national law implementing Union law, an obligation to make data available to a data recipient does not oblige the disclosure of trade secrets within the meaning of Directive (EU) 2016/943.'

Contextually, it does not become clear why reference is made to Article 6 which – contrary to Article 4 and Article 5 – does not contain an obligation to make data available but concerns the obligations of the third-party recipient. Even though Article 4 (3) and Article 5 (8) might fall under the passage 'unless otherwise provided', the wording should be verified and – if necessary – corrected. In our opinion, a reference to Article 5 that imposes the obligation to make data available to third parties would be logical here (cf. also Article 8 (1): 'where a data holder is obliged to make data available to a data recipient under Article 5').

According to Article 8 (6), an obligation *to make data available* does not oblige to *disclose trade secrets*. Thus, the definition of the term 'disclosure' is key: In light of Article 4 (3) and Article 5 (8) which also use this term, 'disclosure' appears to refer solely to 'making an information available without preserving its confidentiality'. The term disclosure as used in the Trade Secrets Directive is however understood broader, meaning any unauthorised 'transfer' of a trade secret to a third party regardless of whether the information is kept secret or not. Using solely the term 'confidentiality' instead of 'secrecy' which is prerequisite for a protection as trade secret might possibly be interpreted in this direction. To avoid legal uncertainty, these terminological issues should in any case be clarified unambiguously, for instance by adding definitions of the respective terms ('disclosure' in the sense of the Data Act, 'confidentiality' in the sense of the Data Act) in Article 2 or defining them at least in the Recitals.

Article 8 (6) furthermore seems to address solely trade secrets of the *data holder* as the user having authorised the third party to access the respective data should not be able to invoke the protection of his/her trade secrets. A respective clarification should also be added ('trade secrets of the data holder').

iii. Other possible elements of FRAND agreements

Apart from the essential elements laid down in Article 8, other elements of FRAND agreements, such as e.g. cross-licences, where appropriate, should be further analysed and, if necessary and appropriate, be added as additional optional elements to the catalogue of Article 8 or be addressed in the Recitals.

b. Compensation (Article 9)

According to Article 9 (1) data holder and data recipient shall agree on a reasonable compensation for making the requested data available. With respect to micro, small and medium enterprises any compensation 'shall not exceed the costs directly related to making the data available to the data recipient and which are attributable to the request', Article 9 (2). Recital 42 states in this regard: 'These provisions should not be understood as paying for the data itself, but in the case of micro, small or medium-sized enterprises, for the costs incurred and investment required for making the data available.'

E contrario, the compensation to be paid by data recipients which are not SMEs might therefore in principle be calculated not solely on basis of the costs incurred for making the data available.[334] Consequently, reasonable compensation in such cases will have to be agreed upon by the parties and will depend not only on the *market value of the data* in question, but also on the *scope of the use rights* which are granted to the third party in line with the purpose of the sharing request.

As for the FRAND (fair, reasonable and non-discriminatory terms) concept in regard to licences of standard essential patents, it is meanwhile acknowledged that FRAND conditions do not require a specific structure, quota or sum to be paid, but indeed constitute a *range* of possible reasonable compensation schemes as long as the basic structure and agreed upon conditions and percentaged shares are in line with reasonable market practice. Essentially, in patent law, FRAND negotiations mainly require a certain step-by-step notification and negotiation procedure.[335] It is however suggested to evaluate thoroughly if the situation in which data holder and data recipient have to agree on terms and conditions for making available and use of data, is comparable to the established FRAND constellation in patent law. Whereas in patent law the process of FRAND negotiations is initiated *after* an infringement and essentially serves as *ex-post* objection (in order to distinguish legitimate licence seekers from systematic infringers engaged in hold-out strategies), the Data Act requires an *ex-ante* agreement between the data holder and the data recipient, before making the data available as mandated by Article 5. In practice, such an *ex-ante* negotiation process (including a necessary dispute settlement procedure) might have the potential to hinder effective

[334] Recital 31 does however not clearly distinguish: 'It [the proposed Regulation] also allows the data holder to set reasonable compensation to be met by third parties, but not by the user, for any cost incurred in providing direct access to the data generated by the user's product'.

[335] CJEU judgment of 16 July 2015, *Huawei v ZTE*, C-170/13, EU:C:2015:477. See further Leistner, M., 'European Experiences: EU and Germany'; Picht, P., 'FRAND Injunctions: an overview on recent EU case law', *Zeitschrift für Geistiges Eigentum,* 2019, 324.

data sharing, or could be used as an instrument to impede or essentially delay data access by third parties. Anyway, even if reasonable data holders and data recipients negotiate with each other, Article 9 (1) raises intricate and hitherto unsolved issues of judicial price setting which from our viewpoint could only be solved by essentially relying on certain procedural guidance for the price negotiations by the involved parties themselves as any attempt by the courts to set reasonable prices would inevitably be bound to be confronted with substantial information deficits.

c. Dispute settlement (Article 10)

In order to make FRAND negotiations a functional and effective instrument establishing a dispute settlement mechanism is therefore very welcome in any case as this will be the only possibility to make Article 9 (1) workable in practice. Article 10 proposes to establish and certify dispute settlement bodies in the Member States. Hence, the decisive questions are, first, *which* authority in the Member States should be competent for this particular task (possibly the respective competition authorities) and, second, whether in light of potential inconsistencies between the Member States' institutional framework and practice and the resulting potentially prohibitive transactions costs, a *European competent authority* might not be preferable. In any case, there may arise an immense need for dispute settlement procedures in this field and beyond. It might be worth taking into consideration to incorporate respective dispute settlement bodies to the Intellectual Property Offices and Organisations, either on the European (EUIPO, Commission) or on the International (WIPO) level.

d. Technical protections measures and unauthorised use/disclosure of data (Article 11)

According to Article 11 (1) the data holder may apply appropriate technical protection measures in order to prevent unauthorised use of the data and ensure compliance with the obligations provided in the Data Act or in a contractual agreement. This purpose-oriented permission to implement technical protection measures shows parallels to the CJEU's 'UsedSoft' judgement in which the Court extended the exhaustion principle to the sale of *digital* program copies subject to the Computer Programs Directive: In the decision, the CJEU deemed it justified that a rightholder implements technical protection measures in order to control that the first acquirer's digital copy is made unusable when reselling it to a second acquirer – but solely for this particular purpose.[336] The second sentence of Article 11 (1) introduces a further limitation for avoiding an excessive use of technical protection measures for impeding the right to share data pursuant to Article 5. As a result of the interplay between the two sentences, the 'reasonableness' or proportionality of the technical protection measures implemented by the data holder can be adequately evaluated. Against this background, Article 11 (1) seems to be a well-balanced solution with respect to technical protection measures.

Article 11 (2) specifies further safeguards against the unauthorised use or disclosure of the received data by the third party. These provisions will apply cumulatively to the already existing protection framework under the Trade Secrets Directive and any applicable legal remedies according to national contract and torts law. Nonetheless, since these rules will vary across the Member States, these additional protective provisions seem consequent, necessary and proportional in particular also to assure the protection of existing factual positions relating to data where such data are not

[336] CJEU, judgment of 3 July 2012, *Used Soft v Oracle*, C-128/11, EU:C:2012:407, paragraphs 79, 87.

protected as trade secrets. Furthermore, the scope of national tort law may vary in the Member States with regard to the protection of non-personal data (e.g. only protection of the integrity of data etc.).

e. Mandatory character of the provisions laid down in Chapter III

Finally, Article 12 (2) mandates that any contractual term 'in data sharing agreements' contradicting the provisions set forth in Chapter III is void. The provision thus highlights again that the right to share data with third parties, including the structural framework for respective obligations of data holders, laid down in Chapter III, has *mandatory* character, even in B2B relations (where the resulting interference with contractual freedom and with free price competition raises certain concerns from our viewpoint).

4.3. Unfair terms related to data access and use between enterprises (Chapter IV)

Article 13 introduces a general 'fairness test' for B2B contract terms concerning the access to and use of data or the liability and remedies for the breach or the termination of data related obligations which have been 'imposed' on micro, small or medium-sized enterprises. If a contractual term is deemed unfair, it shall not be binding on the SME. In order to identify a contract term as 'unfair', Article 13 provides a general clause, complemented by non-conclusive 'black' and a 'grey' lists.

4.3.1. Scope

a. Terms affected by Article 13

Pursuant to Article 13 (1) contract terms concerning (a) access and use of data or (b) liability and remedies for breach or termination of data related obligations are subject to the fairness test. Recital 53 supports the definition of the scope of the fairness test with the argument that these elements of a contract are related to 'making data available'. While regulating the first category of terms (concerning access and use of data) can be seen as logical consequence of the objective to provide basic rules for data access and use, addressing terms concerning liability and remedies for breach or termination of data related obligations goes partly beyond data access-specific aspects. All Member States' laws naturally already foresee differentiated instruments for addressing a breach of a B2B contract and actually it can be assumed that all Member States' laws also contain general civil law provisions on the voidability at least of excessively one-sided clauses in B2B contracts (such as at least the general principle of good faith). In addition, the Unfair Terms Directive[337] provides a general framework of protection against unfair contract terms for B2C relations. Therefore, it should be (re-)considered carefully whether introducing an obligatory B2B fairness test for terms concerning *liability* and *remedies* for breach of contract is actually needed and justified due to data access-

[337] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts (hereinafter 'Unfair Terms Directive').

related considerations. To be sure, a number of Member States' laws[338], such as German law, contain such B2B contract unfairness control provisions; however, mandatory contract law always also causes costs[339] and might – in singular situations – also prevent effective data access and sharing, where e.g. a certain data quality cannot be warranted by the data holder, while the prospective data recipient would be willing to accept this in certain non-sensitive areas.

According to Article 13 (7), the fairness test does not apply to contractual terms defining the main subject matter of the contract or determining the price to be paid. In light of the freedom of contract, excluding these terms is consistent and reasonable (and also contextually in line with the conception of the Unfair Terms Directive). In addition, when designing contracts for data sharing, precisely the definition of the concrete subject matter, the conditions for conformity of the data and the price are highly challenging as established standards and criteria are not applicable to data and actual information problems are still substantially present in the markets. However, the contextual interplay with Article 13 (3) (c) should be clarified: If the definition of the subject matter of the contract is excluded from the unfairness control, why should a clause which enables the data provider to determine conformity (which according to general principles and also because of Article 13 (2) would have to be done in line with good faith, good commercial practice and fair dealing anyway) *always* be considered as unfair and therefore non-binding?

b. Contractual terms being 'unilaterally imposed'

As core requirement of Article 13, the respective contractual terms have to be unilaterally imposed on a micro, small or medium-sized enterprise. According to the definition in Article 13 (1) and (5), a term has been imposed if 'it has been supplied by one contracting party and the other contracting party has not been able to influence its content despite an attempt to negotiate it'.

In regard to this scope and definition, we suggest at least one amendment: It should be specified that the fairness test does not apply to constellations in which a *micro or small business* is the *imposer* of a contract clause covered by Article 13 (1) – this is because in such situations, from our viewpoint, the requirement of a stronger bargaining position cannot always be assumed to be given, e.g. if a micro- or small-sized enterprise (as data provider) negotiates with an SME (as data recipient) and insists on certain clauses because these are essential for effectively staying in business due to the very small size and limited capacity of the small-sized data provider. According to Recital 51 and 52 the fairness test is designed to address situations in which the stronger bargaining position of one party poses the risk of agreements to the detriment of the 'weaker' party (in particular SMEs and smaller businesses) resulting in a 'take-it-or-leave-it' decision on the side of the weaker party. Accordingly, the new unfairness test provided by Article 13 should not apply in cases where the party 'imposing' the contract clause is a micro or small-sized enterprise, because – absent a market dominant position which will be rather seldom in such cases and which would give rise to control of abusive behaviour under EU competition law anyway – the required imbalance of bargaining position seems overwhelmingly unlikely.

---

[338] See Commission Staff Working Document, *Impact Assessment Report*, Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), SWD(2022) 34 final, 2022, p. 170 ('slight majority of Member States').

[339] Commission Staff Working Document, *Impact Assessment Report*, Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), SWD(2022) 34 final, 2022, pp. 45 et seq.; cf. Deloitte and others, *Study to support an Impact Assessment on enhancing the use of data in Europe*, pp. 271, 276 et seq.

Further, from our viewpoint, the question whether and to which extent and, *if at all*, in which particular way the fairness test pursuant to Article 13 should apply with respect to multi-party data sharing networks/pools or – more general – to *multilateral agreements* at the moment remains unanswered by the Data Act. Certainly, if the unfairness test was applied to multilateral agreements and contract negotiations, the definition of a 'unilaterally imposed' term would have to be adjusted or complemented accordingly. In fact, the concept of 'unilaterally imposed'-terms seems hardly workable in larger multi-party network contracts. As already indicated above, reconsidering the role of sharing networks and multipolar settings within the framework proposed by the Data Act seems necessary (unless these agreements shall be excluded from the scope altogether) since diverse provisions are not suitable for cooperative models and multipolar settings.

4.3.2. General clause (unfairness test), Article 13 (2)

According to the general clause contained in Article 13 (2), a term is unfair if 'its use grossly deviates from good commercial practice in data access and use, contrary to good faith and fair dealing'. The terms listed in Article 13 (3) and (4) are (non-conclusive) examples of deviating from good commercial practice and shall therefore serve as a 'yardstick to interpret the general unfairness provision' (see Recital 55). Relying on the principles of 'good faith' and 'fair dealing' is in line with existing soft law principles.[340] Due to its nature as general clause, Article 13 (2) leaves broad leeway for its interpretation and further specification. Certainly, in line with our cautious approach above (see 4.3.1.b) this test should be construed very narrowly, cf. also Recital 54. Contextually, the comparison to Article 3 (1) Unfair Terms Directive ('significant imbalance') already illustrates that stricter criteria will have to be applied in the context of Article 13 (2) ('gross deviation from good commercial practice, contrary to good faith and fair dealing'); one should even consider to also add a sharpened version of the condition according to Article 3 (1) Unfair Terms Directive and thus to cumulatively require a gross imbalance in the parties' rights and obligations arising under the contract as a result of the unfair term.

4.3.3. 'Black list', Article 13 (3)

The terms listed in Article 13 (3) shall generally qualify as *unfair*, thus, the provision has the character of a 'black list'. The three addressed cases, (a) exclusion or limitation of liability for intentional acts or gross negligence, (b) exclusion of remedies in case of non-performance or of liability for contractual obligations and (c) unilateral determination of conformity or interpretation of any term, at first glance do not seem to address data-specific needs, but rather general contract law issues. With respect to B2C relations, comparable terms are already contained in the Unfair Terms Directive.[341] The terms listed as generally unfair in Article 13 (3) construe a similarly strict standard for B2B relations. Since comparable provisions are contained in the Unfair Terms Directive as a general instrument for B2C contracts, this underlines the observation that Article 13 (3) does not touch upon data-related problems in the first place. But, as a result of the resulting strict liability standards, the provision might pave the way for enhancing *data quality*. As stated by Recital 28, the data holder has to ensure that 'the data made available to the third party is as accurate, complete,

[340] E.g. Articles 1:201 and 4:110 Principles of European Contract Law (PECL); Articles 2 and 86 Common European Sales Law (CESL).

[341] Unfair Terms Directive Annex 1 (b) and (m). Liability for intentional acts or gross negligence is equally covered by lit. b, see Loos, M. and Luzak, J., *Update the Unfair Contract Terms directive for digital services*, p. 24.

reliable, relevant and up-to-date'. While this consideration seems valuable for guaranteeing the enforcement of data access rights, strict liability standards could also result in certain chilling effects when in other (voluntary) data sharing constellations information on the provenance of data, their quality, type, size, or content is lacking, the data holder might not be willing to carry the risk of being held liable. In that regard, we have already emphasised that in particular for such situations the contextual relationship to Article 13 (7) should be clarified; it is typical for data-related agreements that the very subject matter of the contract will have to be defined by the parties – therefore, the entire actual impact of Article 13 (3) will very much depend on the question, how Article 13 (7) is understood in that regard.

4.3.4. 'Grey list', Article 13 (4)

Article 13 (4) provides a 'grey list' of terms which are presumed unfair. In contrast to Article 13 (3), the terms contained in Article 13 (4), and particularly lit. (b) to (d), are tailored more specifically to data access and use. In general, these terms show certain parallels to the attempts to modernise the Unfair Terms Directive for B2C relations in the digital age.[342] Lit. (a) can be seen as logical pendant to Article 13 (3) (b), as it is directed to terms 'inappropriately' limiting remedies or liability for non-performance, hence, to a less invasive term. As far as the rather general provision of Article 13 (3) (b) is deemed necessary and justified, the same will hold true for Article 13 (4) (a). As for Article 13 (4) (b) and (c), we have already pointed out that these provisions are of central importance for providing a balanced relationship between different data co-generators and in particular Article 13 (4) (c) on the possibilities to use, capture, access, control or exploit data, should even be generalised, strengthened and complemented with certain procedural rules (in order to support the effective upstream sharing of data as well, cf. above 4.2.3.e). The wording of Article 13 (4) (d) might be refined as the term 'copy of the data' is ambiguous, especially in light of Article 15 (3) GDPR and its intensely discussed scope.[343] While Article 13 (4) (e) seems at first glance to be of a more general nature,[344] due to the identified interoperability and portability issues, guaranteeing sufficient time and possibilities for switching, is a consequent complementary approach which indeed addresses certain data contract related problems in the markets.

4.3.5. Summary

Under the assumption that a mandatory unfairness test for B2B contracts on data sharing is needed and justified, Article 13 establishes a legally coherent and workable structure. In particular, it has to be highlighted that in the interplay with Article 5, the unfairness test strengthens and safeguards the data holder's position in regard to third parties significantly.

However, in our opinion it should be reconsidered whether the proposed fairness test – which is based on data access-related considerations – should also extend to terms concerning *liability* and *remedies* for breach of contract. In any case, it should be specified that Article 13 does not apply where a *micro or small business* 'imposes' a contractual clause on the other party as, from our viewpoint, a stronger bargaining position cannot be assumed 'by default' in such constellations.

---

[342] See in this regard e.g. Loos, M. and Luzak, J., *Update the Unfair Contract Terms directive for digital services*.

[343] In this regard see European Data Protection Board, *Guidelines 01/2022 on data subject rights – Right of access*, p. 12 et seq.

[344] Cf. the provision in the Unfair Terms Directive, Annex 1 (g).

Also, it should be considered to add the condition that a gross imbalance in the parties' rights and obligations arising under the contract must be the result of the unfair term. In addition, the role of the unfairness test in *multilateral agreements* has to be examined thoroughly and, at best, defined in the legal text. Furthermore, the contextual relation between Article 13 (3) (c) and Article 13 (7) should be further clarified.

4.4. Making data available to public bodies based on exceptional need (Chapter V)

Chapter V (Articles 14–22) regulates B2G data access and use rights in situations of exceptional need. The provisions establish a procedural and substantive framework for allowing data access and use in this particular case group.

4.4.1. Scope

According to Article 14 (1) the data holder has, upon request, the obligation to *make data available* to a public sector body or to a Union institution, agency or body demonstrating an exceptional need to *use* the data. As regards the *material* scope, the provisions thus cover both the *access* to and the *use* of the data requested by the public body.

As proposed in Article 14 (2), small and micro enterprises should be exempted from the obligation to make data available to public bodies. Whereas this limitation is coherent with the regulatory concept of the Data Act of excluding small and micro enterprises widely from obligations to make data available, we would suggest that in the specific situations addressed by the provisions in Articles 14 et seq. data access and use rights are also justified vis-à-vis small and micro-sized enterprises. The provisions apply in case of exceptional need and might therefore, in particular in case of a public emergency, require broadest possible access to data including data held by small and micro-sized enterprises. Expressly excluding such enterprises in this context might even give rise to dysfunctional *e contrario* arguments against the application of necessary and proportionate national access rules vis-à-vis small and micro-sized enterprises in such cases. In addition, compared to the B2C and B2B access, use and sharing rights proposed in Articles 4 and 5, making data available to public bodies in exceptional situations does not harm the market position of small and micro enterprises in a comparably intensive manner.

4.4.2. Conditions for making data available

The conditions under which public bodies may request data access and use from a data holder are defined in Article 15. The three case groups, (a) response to a public emergency, (b) prevention of or recovery from a public emergency and (c) – under further prerequisites – fulfilment of a specific task in the public interest explicitly provided by law, are defined and specified adequately from our viewpoint (although we have noted and considered that the term 'public interest' as reason for B2G data access has been criticised in the context of the Impact Assessment[345]).

[345] See for instance Verband der Automobilindustrie, *Position Data Act – Hinweise aus Sicht der Automobilindustrie zur EU-Digitalpolitik*, p. 4.

Article 17 lays down further requirements for the request of the public body. Both the content of the request as defined in Article 17 and the procedure on the data holder's side as specified in Article 18 reduce the data holder's burden to a proportionate degree: As the request has to specify the requested data, demonstrate the exceptional need, define the purposes and name the legal basis (Article 17 (1)), the data holder obtains precise information (also in regard to possible judicial redress). With regard to the scope of the request, the proportionality test in Article 17 (3) (b) and the 'balancing of interest' clause contained in Article 17 (3) (c) provide sufficient leeway for taking into account the data holder's legitimate interests and thus allow to achieve balanced and proportionate results. In addition, the data holder has the possibility to decline the request where the requested data is not available or where the data has already been provided, see Article 18 (2) and (3).

The obligations of the public body as data recipient are designed along the lines of those of the data recipient in case of Article 5: Article 19 (1) obliges the receiving public body to use the data solely for the requested purposes[346] and to delete the data when they are no longer necessary for these purposes. Information (potentially) protected as a trade secret should solely be disclosed where strictly necessary for the requested purposes and under the condition that the public body takes appropriate measures to maintain the confidentiality, see Article 19 (2).

By contrast, potential conflicts with the Database *sui generis* right are not expressly addressed by the provisions in Chapter V. In this regard, Recital 63 states as follows: 'In case the sui generis database rights (…) apply in relation to the requested datasets, data holders should exercise their rights in a way that does not prevent the public sector body and Union institutions, agencies or bodies from obtaining the data, or from sharing it, in accordance with this Regulation.' This Recital corresponds to the provisions on the sui generis right contained in the Open Data Directive and the proposed Data Governance Act (see above 3.1.3 and 3.1.6). It would – all the more in light of this parallel – certainly be preferable to introduce a respective provision to the Data Act instead of a mere non-binding Recital. Also, since the interplay of the Database sui generis right and the Open Data Directive (and its predecessor) have proven to be somewhat problematic in Member States' practice and in light of the carefully limited character of the B2G data access and use mechanism foreseen in Chapter V, one should consider whether it would not be more effective to straightforwardly add a respective exception from protection to the Database sui generis right to prevent practical difficulties with the application of the rather flexible standard laid down in Recital 63.

4.4.3. Compensation

Pursuant to Article 20, the data holder has to be compensated for making data available in case of Article 15 lit. (b) and (c), whereas data access and use that is requested for responding to a public emergency, lit. (a), shall be free of charge. With regard to the Impact Assessment, it had been stressed that an adequate compensation mechanism for B2G had to be implemented for all case groups of data access in the public interest.[347] According to Article 20 (2), the compensation of the data holder shall not exceed 'the technical and organisational costs incurred to comply with the request including, where necessary, the costs of anonymisation and of technical adaptation, plus a

[346] See further Recital 65 according to which data made available to a public body 'should only be used for the purpose for which they were requested, unless the data holder that made the data available has expressly agreed for the data to be used for other purposes'.

[347] Cf. Verband der Automobilindustrie, *Position Data Act – Hinweise aus Sicht der Automobilindustrie zur EU-Digitalpolitik*, p. 4. Also highlighting this aspect, Perarnaud, C. and Fanni, R., *The EU Data Act – Towards a new European data revolution?*, p. 4.

reasonable margin'. Calculating the data holder's compensation on this basis takes into account the legitimate interests of both sides in a balanced way. Most importantly, the interest of the data holder to be reimbursed for the costs incurred for preparing data for sharing, is covered adequately. Even though Article 21 allows the receiving public body to share the requested data for carrying out scientific research or analytics, the scope of the provision is strictly limited to non-profit institutions or public-interest missions recognised by law. As a result, legitimate interests of the data holder do not appear to be harmed inadequately, in particular as the data-receiving institutions themselves have to comply with the obligations set forth in Article 19.

4.4.4. The role of personal data

As far as possible, the request shall be limited to non-personal data (Article 17 (2) (d)), whereas personal data shall only be included where strictly necessary (Recital 64). The extraordinary situations defined as exceptional need in Article 15 will however often also justify a need for personal data, all the more as the GDPR itself provides for respective legal bases, e.g. Article 6 (1) (d) and (e), Article 9 (g) or (i) GDPR. If a public body requests personal data, the data holder is obliged to take reasonable efforts to pseudonymise the data, insofar as the request can be fulfilled with pseudonymised data (see Article 18 (5)). It is of particular importance that the provision refers solely to *pseudonymisation* instead of requiring *anonymisation* (as Recital 64 does) as due to the huge amount of available data and the advanced analytical methods it has become technically nearly impossible to anonymise data. However, the attempt to foster interoperability and the development of technical standards (provisions in Chapter VIII) should be used to incorporate technical but also organisational measures for the anonymisation of data.[348]

4.4.5. Competent authorities and cooperation

Article 22 aims at implementing a framework of mutual assistance and cross-border cooperation between public sector bodies and Union institutions, agencies and bodies and the competent authorities. The structure shows certain parallels to the one-stop shop approach followed by the GDPR (Articles 60 et seq. GDPR). It is in principle desirable to establish such a consistent cooperation structure between the different bodies and authorities in order to minimise the effort on both sides. In practice, and particularly in the beginning, establishing a functioning and effective cooperation structure might however be practically challenging. For instance, the cooperation mechanism set forth in the GDPR has led to significant difficulties in practice, even concerning 'simple' problems such as the preferred language. It might therefore be preferable to rely on already *established structures of cooperation* and limit the number of involved institutions.

4.4.6. Summary

Grosso modo speaking, the provisions on making data available to public bodies based on exceptional need constitute a well-balanced and equitable framework. In particular, the provisions comply with the general principles defined by the High-Level Expert Group on Business-to-Government Data Sharing (see above 3.1.8.b). The conditions for an 'exceptional need' are defined narrowly and sufficiently specific. Due to the requirements for a detailed request of the public body

[348] See above 3.3.3.

including a proportionality test and the need to respect the data holder's legitimate aims, there is sufficient leeway for balancing the interests of both sides. The use of the data by the public body is limited to the requested purposes, but at the same time allows 'societal participation' as (non-profit) research activities can be carried out. In addition, the compensation foreseen for the data holder, except for the response to a public emergency (the Impact Assessment has criticised this limitation so that particular attention should be paid to this issue in the further legislative process), seems reasonable. As a result, the proposed framework creates mutual beneficial conditions for B2G data access and use under sufficiently transparent circumstances justified by an exceptional public interest. We would suggest to reconsider whether the provisions should also be extended to small and micro-sized enterprises. In addition, as we have suggested in other contexts before (see above 3.3.3), strategies for developing workable anonymisation standards should be placed on the agenda.

4.5. Switching between cloud and edge services (Chapter VI)

4.5.1. Scope: B2C and B2B

The Free Flow of Non-Personal Data Regulation pursued a self-regulatory approach for cloud service providers in order to establish efficient portability (see above 3.1.2). However, the developed SWIPO Codes of Conduct were of only very limited effect and have not significantly contributed to enhanced data portability between cloud service providers.[349] As a result, the newly proposed provisions in Chapter VI of the Data Act are *mandatory* in nature and shall apply to B2C and B2B relations alike.

The addressed 'data processing services' are defined as digital services enabling 'on-demand administration and broad remote access to a scalable and elastic pool of shareable computing resources of a centralised, distributed or highly distributed nature', see Article 2 (12). Therefore, both 'classic' cloud services providing Infrastructure as a service (IaaS) and other formats such as for instance Software as a Service (SaaS) or Platform as a Service (PaaS) are entailed (see Recital 71), but certain obligations do not apply to all these services alike (see below 4.5.3.a).

The provisions for facilitating cloud switching follow the objective to *reduce lock-in effects and foster competition* by enabling the user to port data easily from one provider to another. Whereas this argumentation is warranted with respect to B2C relations, the implementation of mandatory rules for B2B relations requires additional justification. Even though the voluntary, self-regulatory approaches have not led to the expected results, this does not per se prove sweeping market failure or information asymmetries in the B2B cloud sector.[350] Rather it seems, that certain technical and organisational (and other practical) barriers to cloud switching have not yet been overcome in actual business practice.

Therefore, from our viewpoint, it has to be ensured that the proposed provisions on switching do *not increase the market entry barriers for SMEs* in a way being detrimental to workable competition in

[349] See also Recital 70 Proposal for a Data Act, COM(2022) 68 final, 2022.

[350] However, we note that the 'Cloud Switching Study' has recommended to introduce a new portability right as most efficient instrument (IDC and Arthur's Legal, *Switching of Cloud Services Providers*, Study prepared for the European Commission, Executive Summary, p. 8) and that detrimental costs in particular for SMEs have been observed (EY, *Study on the economic detriment to small and medium-sized enterprises arising from unfair and unbalanced cloud computing contracts*, p. 79 et seq.).

the relevant markets. Implementing the necessary technical infrastructure for facilitating data portability requires high costs and significant efforts from the providers. As a consequence, – and comparable to the discussion on Article 20 GDPR – the mandatory rules for cloud switching might have the potential to consolidate the position of powerful market actors and rise the barriers for new market entrants. In short: Too strict a standard might risk to lead to dysfunctional results as on the long run the main structural objective should be to establish more intense competition in the markets for cloud and edge services. In addition, the most central practical problem of lacking interoperability and technical standards for data formats and APIs remains and – despite the provisions in Chapter VIII – will remain unsolved until respective standards come into existence.

In conclusion, from our viewpoint it should be considered to foresee an exception for SMEs as providers, applying at least in B2B relations.[351]

4.5.2. Overlaps with the proposed Digital Markets Act

Due to the broad scope of the portability rights in Articles 23 et seq., overlaps with the proposed Digital Markets Act and particularly Article 6 (1) (h) of the Digital Markets Act applying in relation to gatekeepers will arise.[352] Article 6 (1) (h) of the proposed Digital Markets Act will, inter alia, be of significant importance where service providers rely on cloud services by a third-party provider. Pursuant to Recital 73, the provisions of the Data Act shall apply simultaneously in such cases. The most important difference between the two provisions is that Article 6 (1) (h) Digital Markets Act provides explicitly for 'continuous and real-time' access. While this difference can be justified with the limited scope of the Digital Markets Act (only addressing gatekeepers), nonetheless certain inconsistencies remain. The Data Act does not cover real-time portability, but extends to volunteered and observed data including meta-data, configuration parameters, security settings, access rights and logs (Article 24 (1) (b)). Thus, in some respects the scope of the provision proposed in the Data Act (currently for any business in the sector, including SMEs) is even *further-reaching* than the Digital Markets Act's obligations of gatekeepers.

4.5.3. Obligations of the data processing provider

a. Instruments against 'circumvention'

In line with the objective to practically facilitate switching between cloud and edge services on all levels, the obligations laid down in Article 23 (1) (addressing not only the porting of data itself (lit. c) but also complementary aspects such as the contract termination and conclusion of a new contract) aim to prevent a circumvention of the switching possibilities by way of additional commercial, technical, contractual and organisational obstacles.

In particular, as effective data porting requires a certain degree of technical interoperability, Article 23 (1) (d) imposes the duty of the provider to remove obstacles inhibiting customers from

---

[351] Cf. Crémer, J., de Montjoye, Y. and Schweitzer, H., *Competition Policy for the digital*, p. 58, with regard to market power. In a similar vein, IDC and Arthur's Legal, *Switching of Cloud Services Providers*, Executive Summary, p. 8, suggesting to 'include some provisions for excluding new or leading-edge cloud offerings from the requirement for portability, as long they saw evidence that the providers and its associated third-party ecosystem would within a reasonable timeframe create tools and standards for end-user organizations, resulting in the new offering with industry-standard levels of portability'.

[352] The proposed Digital Markets Act should explicitly apply to cloud service providers, see Article 2 (2) (g) of the proposal.

maintaining functional equivalence in the environment of another service provider. In line with the objective of Article 23, this practically central provision therefore contains an additional safeguard against hampering (legal) switching possibilities through imposing technical protection measures, uncommon data formats etc. which would factually prevent the use of another service provider. This indeed seems adequate and reasonable.

As to the details, Article 23 (1) (d) refers to Article 26. However, Article 26 (1) seems to extend the obligation of the data processing service provider (from an obligation not to erect any technical obstacles in regard to existing and future solutions for technical interoperability) into a genuine *warranty* ('shall ensure') that the customer can enjoy functional equivalence in the use of the new service. Desirable as this result may be, such a far-reaching obligation cannot be imposed on the original services provider (alone) as, first, it is practically impossible for the original service provider to control and enable functional equivalence (in the use of the new service) and, second, such duty would therefore (and in light of the fact that technical solutions to enable such far-reaching technical interoperability do not exist yet, and, arguably are not even desirable as they might stifle competition on the merits of different functionalities) would amount to a disproportionate burden on the original provider. Therefore, the wording of Article 26 (1) should be aligned with the objective behind Article 23 (1) and limited accordingly.

Leaving aside this particular aspect, the 'layered' model of Article 26, differentiating between the obligations of classic cloud storage service providers (= IaaS, Article 26 (1)) and other services such as SaaS, PaaS or 'XaaS' (Article 26 (2) and (3)), is a reasonable approach. However, it does not become apparent why providers of services in the sense of Article 26 (1) should not be obliged (explicitly) to make open interfaces publicly available and to ensure compatibility, in particular as the development of technical standards will still take some time. In that regard, in the context of Article 26 (1) it should at least be considered whether interfaces necessary for *technical* interoperability in regard to the *infrastructural* elements addressed by Article 26 (1) should not be treated similarly to interfaces under Article 26 (2) and (3).

b. Contractual basis and covered data categories

Article 24 implements the obligation to conclude a *written* (it should be clarified that any electronic form will be sufficient, since Member States' laws might differ on the conditions for what a written executed contract is[353]) contract laying down the rights of the customer and the obligations of the provider in relation to the switching of the service. The clauses' mandatory minimum content defined in lit. (a) to (c) establishes a detailed structure, thus guaranteeing uniform conditions for cloud service customers while at the same time allowing for certain procedural flexibility. Defining concrete timeframes seems to be an efficient instrument to enforce portability in practice; however, it is beyond the qualification, knowledge and experience of the authors, to assess whether a unitary maximum transition period of 30 days is realistic in the majority of cases (although it seems unlikely to us). Anyway, often technical issues will hinder an effective completion (see. 24 (1) (a) (1): 'where technically feasible'), in which case the procedural duties and extended time period of Article 24 (2) will apply.

[353] Article 1:301 (6) Principles of European Contract Law (PECL) might serve as a guideline according to which written statements 'include communications made by telegram, telex, telefax and electronic mail and other means of communication capable of providing a readable record of the statement on both sides.'

Pursuant to Article 24 (1) (b) at a minimum, 'all data imported by the customer, all data and meta-data created by the customer and by the use of the service, including, but not limited to, configuration parameters, security settings, access rights and access logs' shall be covered. Whereas this categorisation at first sight amounts to a comprehensive scope comprising volunteered and observed data of the customer, it has a far-reaching notion in detail. In particular configuration parameters, security settings, access rights and logs go beyond the basic understanding of 'portability'. However, in light of the proposed concept of guaranteeing the user to enjoy 'functional equivalence', allowing to port even these data categories is at least a coherent and logical approach.

According to Article 25, data processing service providers will have the possibility to charge a fee for the switching process during a 'sunset period' which is not yet defined. Article 25 (4) empowers the Commission to introduce a monitoring mechanism for switching charges by means of delegated acts (see Article 38). On principle, the suggested three step solution (negotiated fee, cost covering fee, no fee) is a proportionate step-by-step approach. Nonetheless, we note that switching of services (in particular in B2B settings) is a highly complex, burdensome and cost-intensive task in practice. Although this is beyond our expertise, we do not expect that any short-term solution for generally organising this effectively on the technical and organisational level will emerge in the markets anytime soon.

4.5.4. Summary

On principle, switching provisions can serve as a tool to enhance competition by alleviating lock-in problems in regard to cloud services. The main challenge consists in establishing an effective regulatory framework, if and where necessary, without at the same time imposing significant market entry barriers for SMEs, thus stifling the very competition which is needed in cloud service markets. Therefore, we propose to consider an exception for SMEs as data processing service providers, at least in B2B relations.

Furthermore, the concept of 'functional equivalence' should be clarified by focussing on its justified core content, laid down in Article 23 (1), and the relation to the portability right in Article 6 (1) (h) Digital Markets Act should be addressed. To an extent comparable to the user's right to share data with third parties (Article 5), effective enforcement of the portability right could be fostered by allowing the transfer or fiduciary exercise of these rights, e.g. by an intermediary or directly by the 'new' service provider.[354]

4.6. International contexts non-personal data safeguards (Chapter VII – Article 27)

Article 27 lays down the obligation of data processing service providers to take reasonable technical, legal and organisational measures to prevent access to non-personal data which are held in the Union in international contexts. Due to the broad definition of providers offering 'data processing services', cloud storage providers are included; this shall lead to an efficient protection of data which is not stored in in-house infrastructure. The conditions for transferring or making data available foreseen in Article 27 (3) appear to provide an adequate and structured framework for protecting

[354] Cf. Metzger, A., 'Access to and porting of data under contract law: Consumer protection rules and market-based principles', p. 297 et seq.

non-personal data against inadequate international transfer or governmental access as far as this is at all possible for an instrument of Union jurisdiction.

Due to the closeness to the proposed Data Governance Act, it makes sense that the 'European Data Innovation Board', to be established according to Article 26 of the Data Governance Act, shall advise and assist the Commission according to Article 26 (3) of the Data Act. Article 26 (4) and (5) which are modelled on provisions originally established for personal data (data minimisation) establish the principle to make the minimum amount of data available and to inform the data holder about access requests.

4.7. Interoperability (Chapter VIII)

The provisions on interoperability and standards in Articles 28–30 do notably not establish *generally* applicable technical requirements for service providers.

Article 28 solely addresses 'operators of data spaces', thus, the particular case of 'common European data spaces'.[355] The requirements set forth in Article 28 (1) reflect the core prerequisites identified for establishing effective data portability and data transfers (see above 3.3.5). Therefore, it would in principle be desirable to apply the requirements to *all* providers under an obligation to make data available.

However, with regard to service providers, Article 29 solely addresses 'open interoperability specifications and European standards' which still have to be developed in compliance with the procedure defined in Regulation (EU) No 1025/2012 on European standardisation.[356] According to Article 2 (15) of the Data Act, 'open interoperability specifications' are 'ICT technical specifications, as defined in Regulation (EU) No 1025/2012, which are performance oriented towards achieving interoperability between data processing services'. Since the Regulation on European standardisation sets forth particular rules for the development of European standards, Article 29 is therefore merely a 'policy statement' to kick-start the respective procedure.[357] This is undoubtedly an important first step, but it has to be borne in mind, that as a consequence, technical interoperability problems complicating data sharing and data portability are not resolved yet, which is why the respective portability rules will confront considerable obstacles in practice. Enhancing data interoperability *and* technical interoperability (software tools) is necessary in order to make the existing and envisaged portability, access and sharing rights (and additional voluntary data sharing) work in practice.

Article 30 defines specific requirements for smart contracts, though *no technical standards* either. However, the 'essential requirements' in Article 30 (1) such as the robustness, safe termination and interruption mechanisms, data archiving, continuity and access control establish a reasonable framework corresponding with the standards of information security (confidentiality, integrity, and

[355] European Commission, *A European strategy for data*, COM/2020/66 final, 2020, p. 21 et seq.

[356] Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation.

[357] See Proposal for a Data Act, COM(2022) 68 final, 2022, Explanatory Memorandum, p. 16.

availability). The Commission is furthermore empowered to adopt, by means of delegated acts, common specifications for the essential requirements defined in Article 30 (1).[358]

In sum, the provisions on interoperability implement a comprehensive framework for operators of data spaces, but fall short of establishing conditions for effective data portability, access and sharing as the technical standards still have to be developed. We suggest that the general principles applicable to the operators of European data spaces should in essence be extended accordingly to guide necessary future standardisation processes in regard to cloud portability, data access and data sharing.

4.8. Implementation and enforcement (Chapter IX)

4.8.1. Competent authorities

Articles 31–33 implement the framework for the *public enforcement* of the Data Act. According to Article 31, the Member States shall designate one or more competent authorities for the application and the enforcement of the proposed Regulation. In general, the data protection authorities shall be responsible where personal data is concerned, sectoral authorities where sector-specific regulation applies, and authorities having experience in the field of data and electronic communications services where the provisions on switching between cloud services are at stake. As these sectors have to be distinguished on the one hand, but do undoubtedly overlap on the other hand, it has to be carefully analysed how to assign the competences between the different authorities. The same holds true for distributing the competences between the authorities of the Member States and those on the European level appropriately and without jeopardising the need for a harmonised and coordinated enforcement (see already above, 4.1.1).

In addition, it will have to be considered, at which competent authority (European Authority) to allocate the dispute settlement procedures foreseen in the Data Act in order to make them effectively work in practice (see above 4.1.1).

At a European level ideally one 'meta-authority'[359] should be established, being competent for the enforcement and coordination of all data-related obligations implemented with the entire 'data package'. Such institution could be split in different areas of competence in order to perform the tasks assigned with the Data Act and, for instance, the Data Governance Act, the Digital Markets Act and the Digital Services Act. Underneath the umbrella level of this 'one-stop shop' authority different European and national institutions could exchange information, cooperate and deliver respective elements of necessary decisions. A unique umbrella institution would thus reduce fragmentation and could furthermore be an important reference point for bundling legal and technical expertise. In addition, it might contribute to the envisaged creation of common European data spaces and complement the actions of the 'Support Centre for data sharing'. The 'European

[358] A similar provision is contained in Article 28 (5) for operator of data spaces, but not in Article 29 concerning data processing services in general as this provision requires the formal implementation procedure of *technical* standards. As a result, Article 29 (5) empowers the Commission solely to 'publish' the developed specifications and standards. Recital 76 of the Proposal for a Data Act seems to refer to Regulation (EU) No 1025/2012 (not: 2021) of the European Parliament and of the Council of 25 October 2012 on European standardisation.

[359] See already above 4.1.1; Weizenbaum Institute, *Position Paper concerning Data Act – Inception Impact Assessment*, p. 12.

Competition Network' could serve as a model for designing an efficient cooperation structure between national and European authorities underneath such umbrella 'meta-authority'.[360]

These considerations should also be borne in mind with respect to Article 33 concerning *penalties* for an infringement of the obligations laid down the Data Act. According to Article 33 (1), it is left to the Member States to lay down rules on penalties applicable to infringements of the Data Act. By definition this will lead to different standards within the Member States. In addition, the data protection authorities, for instance, shall remain competent to impose administrative fines for the infringement of the GDPR in the context of the rules for data access, use and sharing contained in Chapter II and III (see Article 33 (3)). All this leads to a considerable risk of *overlapping and parallel enforcement* which might lead not only to *inefficient* (or contradicting) results but also to *chilling effects* due to legal uncertainty and resulting information costs.

4.8.2. Private remedies and enforcement

Comparable to the proposed Digital Markets Act (in regard to which we have criticised this aspect already[361]), the Data Act does not comprehensively address the role of *private remedies and enforcement*. Due to its structure, the Data Act does not follow a strict concept of public enforcement by the competent authorities as, for instance, the GDPR or the Digital Markets Act.

Article 32 (1), stating that '[w]ithout prejudice to any other administrative or judicial remedy, natural and legal persons shall have the right to lodge a complaint, individually or, where relevant, collectively', does expressly *not preclude private remedies* or enforcement. From our viewpoint, it should be clarified (by expressly foreseeing private rights to access and sharing) that *private enforcement is key* for both, the effective workability of the new access and sharing mechanism and the appropriate and proportionate case-by-case specification of the open-ended standards (general clauses) contained in the Data Act. In particular, it also seems necessary to *harmonise* the essential elements of private enforcement, because otherwise there would also be a considerable risk of disharmonisation, not only concerning direct claims by users, but also, for instance, unfair competition law-based actions by competitors under national Member States' laws.[362]

It has to be noted, in this respect, that as for Article 80 (2) GDPR, the CJEU has recently decided that this provision 'must be interpreted as not precluding national legislation which allows a consumer protection association to bring legal proceedings, in the absence of a mandate conferred on it for that purpose and independently of the infringement of specific rights of the data subjects, against the person allegedly responsible for an infringement of the laws protecting personal data, on the basis of the infringement of the prohibition of unfair commercial practices, a breach of a consumer protection law or the prohibition of the use of invalid general terms and conditions, where the data

[360] Cf. Council Regulation (EC) No 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty. See also above 3.1.7.

[361] See Leistner, M., 'The Commission's vision for Europe's digital future: proposals for the Data Governance Act, the Digital Markets Act and the Digital Services Act – a critical primer', *Journal of Intellectual Property Law & Practice*, 2021, p. 782 et seq.

[362] See on the German Unfair Competition Act as an example in the context of the DMA proposal, already Leistner, M., 'The Commission's vision for Europe's digital future: proposals for the Data Governance Act, the Digital Markets Act and the Digital Services Act – a critical primer', *Journal of Intellectual Property Law & Practice*, 2021, p. 782 et seq.

processing concerned is liable to affect the rights that identified or identifiable natural persons derive from that regulation'.[363] Despite the structural differences between the Data Act and the GDPR it might thus be argued, that national law could, for instance, allow consumer protection associations to bring legal proceedings to enforce the obligations laid down in the Data Act in the future. This example alone illustrates that the private law (contract and tort law) approaches in the different national jurisdictions will vary widely and potentially lead to heterogenous results. Therefore, provision of and harmonisation of the essential elements of private remedies is necessary. Moreover, the exact relationship between public enforcement (and respective administrative decisions) and private remedies and proceedings needs to be clarified.

In that regard (and ideally with respect to public enforcement as well), the international dimension of data access, sharing and use markets will also have to be taken into account. Hitherto, the Data Act does not contain express choice of law rules. Particularly for private remedies (which even if they are not foreseen, as we have suggested in the Data Act, will come into play in national law anyway), this aspect will have to be discussed and addressed in the prospective legislative process.

4.8.3. The role of model contract terms

According to Article 34, the Commission shall develop and recommend non-binding model contractual terms on data access and use. Despite its location at the very end of the Regulation, this provision addresses a necessary core instrument for making the Data Act as well as data access, use, sharing and portability on contractual basis in general work effectively in practice. Hitherto, model contract terms for data sharing on contractual basis and on the necessary protection and/or use of trade secrets are lacking. This aspect has been identified as one of the fundamental factors for the current legal uncertainty (see above 2.1.3).

The Data Act has the ambitious objective to reduce legal uncertainty and to provide a common basis for horizontal data sharing. The proposal is based on bilateral contracts as core element, but as long as no model terms for drafting these contracts exist, the legal uncertainty might potentially even increase. In addition, the fairness test for B2B data sharing contracts contained in Article 13 will add an additional level of complexity. Moreover, aspects such as the minimum content for cloud service contracts defined in Article 24 will also call for model contract terms to implement and specify all these requirements in practice. In sum, first and foremost (and actually more pressing than mandatory contract law on certain B2B unfair practices), the development of *model contract terms* for data access, use and sharing (for both B2C and B2B relation) should be pushed forward – so that they, at best, can be provided together with the Data Act becoming effective.

4.9. Database sui generis right (Article 35)

4.9.1. Exclusion of machine-generated data from sui generis protection

The difficult role of the database sui generis right in the context of data access, use and sharing has been comprehensively outlined above (3.2.2.b) where we showed that the database sui generis

[363] CJEU, judgment of 28 April 2022, *Meta Platforms Ireland v Federation of German Consumer Organisations*, C-319/20, EU:C:2022:322, paragraph 84 ; see already Advocate General de la Tour, R., opinion of 2 December 2021, EU:C:2021:979, paragraph 85.

right has the potential to intensify de facto control over data, to aggravate existing access problems and to lead to hold-up issues in certain situations. Taking up on the immense legal uncertainty in regard to the distinction between collection and creation of data,[364] pursuant to Article 35, the sui generis right 'does not apply to databases containing data obtained from or generated by the use of a product or a related service'. Recital 84 states in this regard, that the sui generis right does not apply to such databases as the *requirements for protection* would not be fulfilled. In line with the recommendations of the accompanying Study on the Review of the Database Directive,[365] machine-generated data are hence excluded from the scope of the sui generis right. According to the latter Study, a clear exclusion of machine-generated data contributes to legal certainty, ensures that sui generis rights do not become an obstacle for data sharing and is most efficient since relying on the new infringement test developed by the CJEU in the CV-Online Latvia judgment would currently be too uncertain.

Article 35 identifies sensor and machine-generated data as by-products of another economic activity – namely of the sale, rental or leasing of the product and provision of related services –, so that necessary investments relate to the *mere creation* of data, being irrelevant for the requirement of a substantial investment.[366]

While the explicit clarification that machine-generated data do not fulfil the conditions of the sui generis right seems acceptable as it reduces the significant legal uncertainty in regard to its conditions for protection, the wording of Article 35 should be 'refined': The first part of the provision seems to imply at first glance that the sui generis right should not apply solely where it could interfere with the exercise of the access and use rights set forth in Article 4 and Article 5. Furthermore, it could be expressed more clearly that databases consisting of machine-generated data do not fulfil the requirement of a 'substantial investment in the obtaining, verification or presentation' foreseen in Article 7 (1) of the Database Directive, while they are still within the scope of the Directive so that it is unambiguously clear that no specific protection right shall apply in such cases.[367] Moreover, it would be recommended that at the very least it should be clarified (in the sense of a Union law pre-emption doctrine) that within the scope of the Database Directive, if a given database does not fulfil the conditions for protection, Member States shall be precluded to protect such a database on different grounds (such as *parasitisme* or unfair competition protection against misappropriation, unless additional factors, such as consumer confusion, warrant such additional unfair competition law based protection).[368]

Excluding all databases 'containing' data obtained from or generated by the use of a product or a related service creates the risk to 'rule out' even databases which comprise *inter alia* machine-generated data but were also the result of a substantial investment in the *collection* of data (e.g. investment-intensive sensor systems for environmental data) and where there is sufficient competition in regard to alternatives to collect these data. We had therefore suggested more differentiated solutions in that regard.[369] However, since a bright line rule is needed, the exclusion provision in Article 35 might nonetheless be acceptable and indeed justifiable from our viewpoint.

---

[364] See Proposal for a Data Act, COM(2022) 68 final, 2022, pp. 4, 9.

[365] *Study to Support an Impact Assessment for the Review of the Database Directive*, Final Report, 2022, p. 8.

[366] On this distinction see above 3.2.2.b.i.

[367] Derclaye, E. and Husovec, M., *Why the sui generis database clause in the Data Act is counter-productive and how to improve it?*, p. 2 et seq.

[368] See already above 3.3.1.a.v.

[369] Leistner, M., Antoine, L. and Sagstetter, T., *Big Data,* p. 439 et seq.

Hence, the clarification that machine-generated data does not qualify for protection under the sui generis right solves some of the above-mentioned problems in regard to the conditions of protection by providing for a bright line non-conflict rule. However, many of the problems we have identified in the first part of this study and in earlier publications are not addressed by this very targeted provision.

4.9.2. The Database Directive: additional need for reform

Beyond Article 35 of the Data Act, the most imminent aspects of the database sui generis right which are in need for reform and would require amendments of the Database Directive itself, can be summarised as follows:

First, even though machine-generated data does not qualify for protection under the sui generis right, the *term of protection* of 15 years is far too long also for other types of electronic databases. As recommended above (3.3.1.a.iii) the term should be shortened to a maximum of three years. *Second*, the need for excluding *databases of public bodies* from sui generis protection remains unchanged and is particularly necessary in order to establish coherence with the Open Data Directive (above 3.3.1.a.ii). *Third*, the entire system of exceptions and limitations to the sui generis right calls for a comprehensive reform (see 3.3.1.a.ii) as even with the exclusion of machine-generated data from the sui generis right's scope many databases in a data-driven economy will qualify for protection under Article 7 of the Database Directive; in that context, the new B2G provisions in the proposed Data Act should ideally be complemented with a matching exception to the sui generis right. *Fourth*, Article 35 of the Data Act cannot adequately address hold-up problems with regard to aggregated datasets. Databases protected by the sui generis right can, for instance, arise as an unintended result of a contract-based data sharing network or in the context of an employment relationship. After contract termination, the database sui generis right might consequently be invoked by one of the rightholders, preventing further use of the aggregated datasets. As the sui generis right has therefore significant potential to hamper the use of *aggregated* datasets, a *compulsory licence regime* – as already proposed above (3.3.1.a.vi) – should be introduced to the Database Directive in order to prevent sole-source situations pro-actively.

4.10. Evaluation and review (Article 41), ex-post evaluation plan

Finally, it shall be considered which solutions, e.g. a data collection plan, would allow for an ongoing evaluation of how legal solutions recommended in the study and proposed in the Data Act are implemented and if they are efficient and effective (ex-post evaluation plan).

Article 41 foresees an *ex-post evaluation* of the Data Act by the Commission *two years* after the date of its application. Such evaluation shall particularly assess whether other categories or types of data should be incorporated, certain categories of enterprises as beneficiaries of the data sharing right under Article 5 should be excluded, other situations should be deemed as exceptional needs for the purpose of Article 15, changes in contractual practices of data processing service providers and sufficient compliance with Article 24 can be observed and how switching charges imposed by data processing service providers (Article 25) have developed.

Even though the Impact Assessment Report on the estimated impact of the Data Act from an economic and empirical perspective refers to the year 2028,[370] a more *practice-oriented* evaluation as described in Article 41 two years after the Data Act's date of application is recommendable. Indeed, such clause seems necessary to inject flexibility into the legal instrument which is needed in light of the very dynamic development of the regulated market sector. Article 41 lit. a allows to verify whether the access, use and sharing rights provided for the IoT sector can serve as blueprint for other constellations[371]; lit. b paves the way for a re-evaluation of actual market failures in regard to horizontal data access[372]; lit. c provides the flexibility to take into account new exceptional challenges which potentially arise in the upcoming years; lit. d and lit. e continue the monitoring of cloud switching initiated with the Free Flow Regulation. These aspects in principle reflect central regulatory objectives of the Data Act as well as conceivably necessary adaptations. They therefore provide a coherent basis for its evaluation and possible future adaptation although one might consider in the interest of increased flexibility whether in addition the Commission should also be empowered to make certain necessary mere specifications of open standards in the Data Act by way of delegated acts.

We have also considered which further elements could contribute to an effective evaluation of the Data Act. The collection of empirical data – both ongoing and ex-post – for assessing the effectiveness of the instruments proposed by the Data Act is not an easy task. This is because the scope of the Data Act is very broad, the proposed instruments are of a very variable nature and the foreseen concepts rather generally formulated and not subject to formalised (easily quantifiable) procedures or results, as for instance in the case of patent applications or other industrial property rights where the impact of regulatory changes on innovation can be more easily quantified. Therefore, the only way to assess the Data Act empirically (and possibly on the basis of a data collection plan) would be to choose specific instruments in the Data Act as well as to carefully choose certain very specific industry sectors (within the broad scope of application) to at least exemplify the impact of the act in very particular, carefully limited sectors where empirical quantification might be possible to a certain extent.

[370] Commission Staff Working Document, *Impact Assessment Report*, Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), SWD(2022) 34 final pp. 68 et seq.

[371] On this aspect, see above 4.2.1.a.

[372] See above 4.2.1.b.

REFERENCES

American Law Institute and European Law Institute, AL*I-ELI Principles for a Data Economy – Data Transactions and Data Rights*, ELI Final Council Draft, 2021, available at: https://www.principlesforadataeconomy.org/fileadmin/user_upload/p_principlesforadataeconomy/Files/Principles_for_a_Data_Economy_ELI_Final_Council_Draft.pdf.

Aplin, T., 'Trading Data in the Digital Economy: Trade Secrets Perspective', *Trading Data in the Digital Economy: Legal Concepts and Tools*, Baden-Baden, Nomos, 2017, pp. 59–72.

Argenton, C. and Prüfer, J., 'Search Engine Competition with Network Externalities', *Journal of Competition Law & Economics*, 2012, pp. 73–105.

Article 29 Data Protection Working Party, *Guidelines on the right to data portability*, WP 242 rev.01, 2017.

Atik, C. and Martens, B., 'Competition Problems and Governance of Non-personal Agricultural Machine Data: Comparing Voluntary Initiatives in the US and EU', *Journal of Intellectual Property, Information Technology and E-Commerce Law*, 2021, pp. 370–396.

Benjamin, M., Gagnon. P. and other, 'Towards Standardization of Data Licenses: The Montreal Data License', *ArXiv*, abs/1903.12262, 2019, available at: https://arxiv.org/pdf/1903.12262.pdf.

Bently, L., Derclaye, E. and others, *Study in support of the evaluation of Directive 96/9/EC on the legal protection of databases – Final Report*, 2018, available at: https://op.europa.eu/de/publication-detail/-/publication/5e9c7a51-597c-11e8-ab41-01aa75ed71a1.

Calatrava Moreno and others, *Study to Support an Impact Assessment for the Review of the Database Directive*, Final Report, 2022, available at: https://digital-strategy.ec.europa.eu/en/library/impact-assessment-report-and-support-studies-accompanying-proposal-data-act.

Capgemini Consulting (as part of the European Data Portal), *Creating Value through Open Data: Study on the Impact of Re-use of Public Data Resources*, 2015, available at: https://data.europa.eu/sites/default/files/edp_creating_value_through_open_data_0.pdf.

Centre on Regulation in Europe (CERRE), *Making Data Portability More Effective for the Digital Economy*, 2020, available at: https://cerre.eu/publications/report-making-data-portability-more-effective-digital-economy/.

Chen, C., Frey, C. and Presidente, G., *Privacy Regulation and Firm Performance: Estimating the GDPR Effect Globally*, The Oxford Martin Working Paper Series on Technological and Economic Change, Working Paper No. 2022-1, 2022.

Crémer, J., de Montjoye, Y. and Schweitzer, H., *Competition Policy for the digital era – Final report*, 2019.

Deloitte, *Study on emerging issues of data ownership, interoperability, (re-)usability and access to data, and liability*, Study prepared for the European Commission, 2016.

Deloitte, *GDPR Data Portability and Core Vocabularies*, Study prepared for the European Commission, 2018.

Deloitte and others, *Study to support an Impact Assessment on enhancing the use of data in Europe*, 2022, available at: https://digital-strategy.ec.europa.eu/en/library/impact-assessment-report-and-support-studies-accompanying-proposal-data-act.

Derclaye, E. and Husovec, M., *Sui Generis Database Protection 2.0: Judicial and Legislative Reforms,* 2021, available at: https://ssrn.com/abstract=3964943.

Derclaye, E. and Husovec, M., *Why the sui generis database clause in the Data Act is counter-productive and how to improve it?*, 2022, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4052390.

DORDA Rechtsanwälte GmbH and others*, Study presenting assessments of codes of conduct on data porting and cloud switching*, 2020, available at: https://digital-strategy.ec.europa.eu/en/library/impact-assessment-report-and-support-studies-accompanying-proposal-data-act.

Drexl, J. and others, 'Position Statement of the Max Planck Institute for Innovation and Competition of 26 April 2017 on the European Commission's 'Public consultation on Building the European Data Economy'', 2017, Max Planck Institute for Innovation and Competition Research Paper No 17–08, https://www.ip.mpg.de/en/research/research-news/position-statement-public-consultation-on-building-the-european-data-economy.html.

Drexl, J., 'Designing Competitive Markets for Industrial Data', *Journal of Intellectual Property, Information Technology and E-Commerce Law*, 2017, pp. 257–292.

Drexl, J., *Data Access and Control in the Era of Connected Devices – Study on Behalf of the European Consumer Organisation BEUC,* 2018.

ENISA, *Privacy by design in big data*, 2015.

European Data Protection Board, *Guidelines 4/2019 on Article 25 – Data Protection by Design and by Default,* Version 2.0, 2020.

European Data Protection Board, *Guidelines 02/2021 on virtual voice assistants,* Version 2.0, 2021.

European Data Protection Board, *Guidelines 01/2022 on data subject rights – Right of access*, 2022.

European Law Institute, *Response to Public Consultation on the Data Act*, 2021.

Everis Benelux, *Study on data sharing between companies in Europe*, carried out for the European Commission, 2018, available at: https://op.europa.eu/de/publication-detail/-/publication/8b8776ff-4834-11e8-be1d-01aa75ed71a1/language-en.

Expert Group for the Observatory on the Online Platform Economy, *Work stream on Data*, *Final Report*, 2021, available at : https://platformobservatory.eu/app/uploads/2020/07/ProgressReport_Workstream_on_Data_2020.pdf.

EY, *Study on the economic detriment to small and medium-sized enterprises arising from unfair and unbalanced cloud computing contracts*, Study prepared for the European Commission, Final Report, 2019, available at: https://ec.europa.eu/info/publications/study-economic-detriment-small-and-medium-sized-enterprises-arising-unfair-and-unbalanced-cloud-computing-contracts_en.

Furman, J., Coyle, D. and others, *Unlocking Digital Competition – Report of the Digital Competition Expert Panel*, UK Government, 2019, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf.

Geiger, C., Frosio, G. and Bulayenko, O., 'Text and Data Mining in the Proposed Copyright Reform: Making the EU Ready for an Age of Big Data?', *International Review of Intellectual Property and Competition Law,* 2018, pp. 814–845.

German Data Ethics Commission, *Opinion*, 2019, available at: https://www.bmi.bund.de/EN/topics/it-internet-policy/data-ethics-commission/data-ethics-commission-node.html.

Ginsburg, J., 'Creation and Commercial Value: Copyright Protection of Works of Information', *Columbia Law Review*, Vol. 90, 1990, pp. 1865–1938.

Graef, I., 'The opportunities and limits of data portability for stimulating competition and innovation', *Competition Policy International – Antitrust Chronicle*, 2020, pp. 2–8.

Graef, I., Gellert, R. and Husovec, M., 'Towards a Holistic Regulatory Approach for the European Data Economy: Why the Illusive Notion of Non-Personal Data is Counterproductive to Data Innovation', *European Law Review*, 2019, pp. 605–621.

Graef, I. and Husovec, M., Seven Things to Improve in the Data Act, 2022, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4051793.

Graef, I., Husovec, M. and Purtova, N., 'Data Portability and Data Control: Lessons for an Emerging Concept in EU Law', *German Law Journal,* 2018, pp. 1359–1398.

Graef, I., Husovec, M. and van den Boom, J., 'Spill-Overs in Data Governance: Uncovering the Uneasy Relationship Between the GDPR's Right to Data Portability and EU Sector-Specific Data Access Regimes', *Journal of European Consumer and Market Law*, 2020, pp. 3–16.

Graef, I. and Prüfer, J., *Governance of Data Sharing: A Law & Economics Proposal*, TILEC Discussion Paper Vol. 2021-001, 2021, available at: https://pure.uvt.nl/ws/portalfiles/portal/47589426/2021_001.pdf.

Heinze, C., 'Software als Schutzgegenstand des Europäischen Urheberrechts', *Journal of Intellectual Property, Information Technology and E-Commerce Law,* 2011, p. 97–113.

High-Level Expert Group on Business-to-Government Data Sharing, *Towards a European strategy on business-to-government data sharing for the public interest – Final Report*, 2020, available at : https://op.europa.eu/de/publication-detail/-/publication/d96edc29-70fd-11eb-9ac9-01aa75ed71a1.

IDC and Open Evidence study, *European Data Market Study – Industrial Data Platforms – Key Enablers of Industrial Digitization*, carried out for the European Commission, 2016, available at: https://docs.google.com/a/open-evidence.com/viewer?a=v&pid =sites&srcid =b3Blbi 1ldmlk ZW 5jZS 5jb218ZG93bmxvYWR8Z3g6NjJiZTQ1NTYyZjdlOGNhNg.

IDC and Arthur's Legal, *Switching of Cloud Services Providers*, Study prepared for the European Commission, 2018, available at: https://op.europa.eu/en/publication-detail/-/publication/898aeca7-647e-11e8-ab9c-01aa75ed71a1.

Japanese Ministry of Economy, Trade and Industry (METI), *Contract Guidelines on Utilization of AI and Data*, Version 1.1., available at: https://www.meti.go.jp/english/press/2019/1209_005.html.

Kerber, W., 'A New (Intellectual) Property Right for Non-Personal Data? An Economic Analysis', *Gewerblicher Rechtsschutz und Urheberrecht Internationaler Teil*, 2016, pp. 989–998.

Kerber, W., 'Governance of Data: Exclusive Property vs. Access', *International Journal of Intellectual Property and Competition Law*, 2016, pp. 759–762.

Kerber, W., 'Digital Markets, Data and Privacy: Competition Law, Consumer Law and Data Protection', *Gewerblicher Rechtsschutz und Urheberrecht Internationaler Teil*, 2016, pp. 639–647.

Kerber, W., *Governance of IoT Data: Why the EU Data Act will not fulfill its objectives*, 2022, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4080436.

Kur, A., and others, 'First Evaluation of Directive 96/9/EC on the Legal Protection of Databases – Comment by the Max Planck Institute for Intellectual Property, Competition and Tax Law, Munich', *International Review of Intellectual Property and Competition Law,* 2006, pp. 551–558.

Lee, J. and Li, Y. 'The Pathway Towards Digital Superpower: Copyright Reform in China', *Gewerblicher Rechtsschutz und Urheberrecht Internationaler Teil,* 2021, pp. 861–870.

Leistner, M., 'Legal Protection for the Database Maker – Initial Experience from a German Point of View', *International Review of Intellectual Property and Competition Law,* 2002, pp. 439–463.

Leistner, M., 'Intellectual Property and Competition Law: The European Development from Magill to IMS Health Compared to Recent German and U.S. Case Law', *Zeitschrift für Wettbewerbsrecht*, 2005, pp. 138–162.

Leistner, M., 'Big Data and the EU Database Directive 96/9/EC: Current Law and Potential for Reform', *Trading Data in the Digital Economy: Legal Concepts and Tools*, Baden-Baden, Nomos, 2017, pp. 27–57, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3245937.

Leistner, M., 'European Experiences: EU and Germany', SEPs, SSOs and FRAND – Asian and global perspectives on fostering innovation in interconnectivity, Routledge, 2019, Chapter 15.

Leistner, M., 'The existing European IP rights system and the data economy', *Data access, consumer interests and public welfare*, Nomos, Baden-Baden, 2021, pp. 209–251, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3625712.

Leistner, M., Towards an Access Paradigm in Innovation Law?, *Gewerblicher Rechtsschutz und Urheberrecht Internationaler Teil*, 2021, pp. 925–931.

Leistner, M., 'The Commission's vision for Europe's digital future: proposals for the Data Governance Act, the Digital Markets Act and the Digital Services Act – a critical primer', *Journal of Intellectual Property Law & Practice*, 2021, pp. 778–784.

Leistner, M., Antoine, L. and Sagstetter, T., *Big Data,* Mohr Siebeck, Tübingen 2021.

Lemley, M., 'The Surprising Virtues of Treating Trade Secrets as IP Rights', Stanford Law Review, 2008, pp. 311–354.

Loos, M. and Luzak, J., *Update the Unfair Contract Terms directive for digital services*, Study requested by the European Parliament's Committee on Legal Affairs (JURI), 2021, available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/676006/IPOL_STU(2021)676006_EN.pdf.

Marly, J., 'Der Schutzgegenstand des urheberrechtlichen Softwareschutzes', *Gewerblicher Rechtsschutz und Urheberrecht*, 2012, pp. 773–779.

Martens, B., 'Data access, consumer interests and social welfare – An economic perspective on data', *Data access, consumer interests and public welfare*, Nomos, Baden-Baden, 2021, pp. 69–102.

Martens, B. and others, *Business to business data sharing: an economic and legal analysis*, Digital Economy Working Paper 2020-05, European Commission, Seville, 2020, JRC121336, available at: https://joint-research-centre.ec.europa.eu/publications/business-business-data-sharing-economic-and-legal-analysis_en.

Marsden, P. and Podszun, R., *Restoring Balance to Digital Competition – Sensible Rules, Effective Enforcement*, 2020.

Metzger, A., 'Access to and porting of data under contract law: Consumer protection rules and market-based principles', *Data access, consumer interests and public welfare*, Nomos, Baden-Baden, 2021, p. 287–317.

OECD, *Data-Driven Innovation: Big Data for Growth and Well-Being,* OECD Publishing, Paris, 2015.

OECD, *OECD Digital Economy Outlook 2017*, OECD Publishing, Paris, 2017.

OECD, *Business models for sustainable research data repositories*, OECD Science, Technology and Industry Policy Papers No. 47, 2017, available at: https://doi.org/10.1787/302b12bb-en.

OECD, *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-Use across Societies,* OECD Publishing, Paris, 2019.

Perarnaud, C. and Fanni, R., *The EU Data Act – Towards a new European data revolution?*, 2022, available at: https://www.ceps.eu/wp-content/uploads/2022/03/CEPS-PI2022-05_The-EU-Data-Act.pdf.

Picht, P., 'FRAND Injunctions: an overview on recent EU case law', *Zeitschrift für Geistiges Eigentum*, 2019, pp. 324-333.

Picht, P. and Richter, H., *The Proposed EU Digital Services Regulation 2020: Data Desiderata*, Max Planck Institute for Innovation and Competition Research Paper No. 21-21, 2021, available at: https://ssrn.com/abstract=3925359.

Polański, P., 'Some thoughts on data portability in the aftermath of the Cambridge Analytica scandal', *Journal of European Consumer and Market Law*, 2018, pp. 141–146.

Prüfer, J. and Schottmüller, C., 'Competing with Big Data', *The Journal of Industrial Economics*, 2021, pp. 967–1008.

Reimsbach-Kounatze, C., 'Enhancing access to and sharing of data: Striking the balance between openness and control over data', *Data access, consumer interests and public welfare*, Nomos, Baden-Baden, 2021, pp. 27–68.

Richter, H., 'Zugang des Staates zu Daten der Privatwirtschaft', *Zeitschrift für Rechtspolitik*, 2020, pp. 245–248.

Richter, H., 'Ankunft im Post-Open-Data-Zeitalter', *Zeitschrift für Datenschutz*, 2022, pp. 3–8.

Richter, H. and Slowinski, P., 'The Data Sharing Economy: On the Emergence of New Intermediaries', *International Journal of Intellectual Property and Competition Law*, 2019, pp. 4–29.

Rubinstein, I. and Good, N., 'The trouble with Article 25 (and how to fix it): the future of data protection by design and default', *International Data Privacy Law*, 2020, pp. 37–56.

Samuelson, P., Vinje, T. and Cornish, W., 'Does copyright protection under the EU Software Directive extend to computer program behaviour, languages and interfaces?', *European Intellectual Property Review,* 2012, pp. 158–166.

Schweitzer, H., 'Datenzugang in der Datenökonomie: Eckpfeiler einer neuen Informationsordnung', *Gewerblicher Rechtsschutz und Urheberrecht*, 2019, pp. 569–580.

Schweitzer, H. and Peitz, M., 'Ein neuer europäischer Ordnungsrahmen für Datenmärkte?', *Neue Juristische Wochenschrift*, 2018, pp. 275–280.

Schweitzer, H. and Welker, R., 'A legal framework for access to data – A competition policy perspective', *Data access, consumer interests and public welfare*, Nomos, Baden-Baden, 2021, pp. 103–153.

Sciadas, G. and Stavropoulos, P., *Methodological support to impact assessment of using privately held data by official statistic*, 2021.

Support Centre for data sharing, *Analytical report on EU law applicable to sharing of non-personal data*, 2020, pp. 11 et seq. and pp. 45 et seq., https://eudatasharing.eu/sites/default/files/2020-02/EN_AR%20on%20EU%20law%20applicable%20to%20sharing%20of%20non-personal%20data.pdf.

Support Centre for data sharing, *Report on collected model contract terms,* availabe at: https://eudatasharing.eu/sites/default/files/2019-10/EN_Report_%20on%20Model%20Contract%_20Terms. pdf.

Ueno, T., 'The Flexible Copyright Exception for 'Non-Enjoyment' Purposes – Recent Amendment in Japan and Its Implication', *Gewerblicher Rechtsschutz und Urheberrecht Internationaler Teil*, 2021, pp. 145–152

US Federal Trade Commission, *Protecting Consumer Privacy in an Era of rapid Change*, Report, 2012, available at: https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

Van Eechoud, M., 'A Serpent Eating Its Tail: The Database Directive Meets the Open Data Directive', *International Review of Intellectual Property and Competition Law*, 2021, pp. 375–378.

Van der Burg, S., Wiseman, L. and Krkeljas, J., 'Trust in farm data sharing: reflections on the EU code of conduct for agricultural data sharing', *Ethics and Information Technology*, 2021, pp. 185 - 198.

Verband der Automobilindustrie, *Position Data Act – Hinweise aus Sicht der Automobilindustrie zur EU-Digitalpolitik*, 2021, available at: https://www.vda.de/de/aktuelles/publikationen/publication/data-act.

Vezzoso, S., 'Copyright, Interfaces, and a Possible Atlantic Divide', *Journal of Intellectual Property, Information Technology and E- Commerce Law*, 2012, p. 153–161.

Weizenbaum Institute, *Position Paper concerning Data Act – Inception Impact Assessment*, 2021, available at: https://www.weizenbaum-institut.de/news/weizenbaum-institut-veroeffentlicht-stellungnahme-zur-folgenabschaetzung-des-eu-data-act/.

World Economic Forum, *Personal Data: The Emergence of a New Asset Class*, 2011, available at: https://www.weforum.org/reports/personal-data-emergence-new-asset-class.

All internet sources last accessed on 20 April 2022.

This study analyses recent developments in data related practice, law and policy as well as the current legal framework for data access, sharing, and use in the European Union. The study identifies particular issues of concern and highlights respective need for action. On this basis, the study evaluates the Commission's proposal for a Data Act.
The study is commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs at the request of the Committee on Legal Affairs.

PE 732.266
IP/C/JURI/2021-080

Print ISBN 978-92-846-9406-8| doi: 10.2861/716774| QA-07-22-237-EN-C
PDF ISBN 978-92-846-9405-1| doi: 10.2861/39552| QA-07-22-237-EN-N