DeutscherAnwaltVerein

Position Paper

of the German Bar Association by the Committees IT Law, Intellectual Property and Europe

on the Proposal for a Regulation on harmonised rules on fair access to and use of data (Data Act) COM(2022) 68 final

Position Paper No.: 40/2022 Berlin/Brussels, July 2022

Members of the Committee on IT Law

- Rechtsanwalt Dr. Helmut Redeker (Chair and Rapporteur)
- Rechtsanwalt Dr. Simon Assion, Frankfurt am Main
- Rechtsanwältin Dr. Christiane Bierekoven, Düsseldorf
- Rechtsanwältin Isabell Conrad, München (Rapporteur)
- Rechtsanwalt Dr. Malte Grützmacher, LL.M., Hamburg
- Rechtsanwalt Prof. Niko Härting, Berlin (Rapporteur)
- Rechtsanwalt Peter Huppertz, LL.M, Düsseldorf
- Rechtsanwältin Birgit Roth-Neuschild, Karlsruhe
- Rechtsanwalt Dr. Robert Selk, LL.M. (EU), München

In charge in the Berlin office

- Rechtsanwältin Nicole Narewski

Members of the Committee on Intellectual Property

- Rechtsanwalt Prof. Dr. Jochen Bühling (Chair and Rapporteur)
- Rechtsanwältin Jana Bogatz, München
- Rechtsanwalt Dr. Dirk Bruhn, Hamburg (Rapporteur)
- Rechtsanwalt Klaus Haft, Dipl.-Phys., Düsseldorf
- Rechtsanwältin Dr. Verena Hoene, Köln
- Rechtsanwalt Prof. Dr. Reinhard Ingerl, LL.M., München
- Rechtsanwältin Dr. Andrea Jaeger-Lenz, Hamburg
- Rechtsanwalt beim Bundesgerichtshof Dr. Matthias Koch LL.M., Karlsruhe

Deutscher Anwaltverein
Littenstraße 11, 10179 Berlin
Tel.: +49 30 726152-0
Fax: +49 30 726152-190
E-Mail: dav@anwaltverein.de

Büro Brüssel
Rue Joseph II 40, Boîte 7B
1000 Brüssel, Belgien
Tel.: +32 2 28028-12
Fax: +32 2 28028-13
E-Mail: bruessel@eu.anwaltverein.de
EU-Transparency Register ID number:
87980341522-66

www.anwaltverein.de

- Rechtsanwalt Prof. Dr. Johannes Kreile, München
- Rechtsanwalt Dr. Henrik Lehment, Düsseldorf
- Rechtsanwältin Dr. Birte Lorenzen, Hamburg (Rapporteur)

In charge in the Berlin office

- Dr. Moritz Moelle LL.M.

Members of the Committee on Europe

- Rechtsanwältin Dr. Claudia Seibel, Frankfurt am Main (Chair)
- Rechtsanwältin Béatrice Deshayes, Paris
- Rechtsanwalt Prof. Dr. Christian Duve, Frankfurt am Main
- Rechtsanwalt Prof. Dr. Thomas Gasteyer, LL.M., Frankfurt am Main
- Rechtsanwalt Prof. Dr. Hans-Jürgen Hellwig, Frankfurt am Main
- Rechtsanwalt Dr. Ulrich Karpenstein, Berlin
- Rechtsanwältin Gül Pinar, Hamburg
- Rechtsanwalt Prof. Dr. Dirk Uwer, Düsseldorf
- Rechtsanwalt Michael Jürgen Werner, Brüssel (Rapporteur)

In charge in the Berlin office

- Rechtsanwältin Nicole Narewski

Contact in Brussels:

- Hannah Adzakpa, LL.M.

Mailing List

Germany

Bundesministerium des Innern, für Bau und Heimat
Bundesministerium der Justiz und für Verbraucherschutz
Bundesministerium für Wirtschaft und Energie

Ausschuss für Recht und Verbraucherschutz im Deutschen Bundestag
Ausschuss für Wirtschaft und Energie im Deutschen Bundestag
Ausschuss Digitale Agenda im Deutschen Bundestag

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Die Datenschutzbeauftragten der Bundesländer

Europäische Kommission - Vertretung in Deutschland
Bundesrechtsanwaltskammer
Bundesnotarkammer
Bundesverband der Freien Berufe
Deutscher Richterbund
Deutscher Notarverein e.V.
Deutscher Steuerberaterverband
Bundesverband der Deutschen Industrie (BDI)
Arbeitsgemeinschaft berufsständischer Versorgungseinrichtungen e. V. – ABV
GRUR
BITKOM
DGRI

DAV-Vorstand und Geschäftsführung
Vorsitzende der DAV-Gesetzgebungsausschüsse
Vorsitzende der DAV-Landesverbände
Vorsitzende des FORUMs Junge Anwaltschaft

Europe

European Commission
- Directorate-General for Communications Networks, Content and Technology

European Parliament
- Committee on Industry, Research and Energy (ITRE)

Council of the European Union
Permanent Representation of the Federal Republic of Germany to the European Union
Justizreferenten der Landesvertretungen
Council of Bars and Law Societies of Europe (CCBE)
Bundesverband der Freien Berufe (Brussels office)
European Digital Rights (EDRi)

Press

Frankfurter Allgemeine Zeitung
Süddeutsche Zeitung GmbH

Redaktion NJW
Juve-Verlag
Redaktion Legal Tribune Online / LTO
Redaktion Anwaltsblatt
Juris
Redaktion MultiMedia und Recht (MMR)
Redaktion Zeitschrift für Datenschutz ZD
Redaktion heise online
Agence Europe

The German Bar Association (Deutscher Anwaltverein – DAV) is the professional body comprising more than 61.000 German lawyers and lawyer-notaries in 253 local bar associations in Germany and abroad. Being politically independent the DAV represents and promotes the professional and economic interests of the German legal profession on German, European and international level. The DAV is registered in the Lobby Registry for the representation of special interests vis-à-vis the German Bundestag and the Federal Government under register number R000952.

---

1. Preliminary remarks

The Draft regulation deals with a variety of not necessarily related topics. Among others, these are related to ‘data silos’, ‘data sharing’ or smart contracts. As a result, the motives and objectives of the legislator remain unclear. Art. 3 *et seq*. of the Draft Regulation contain the right of users to access and use data generated by the use of products or related services. These articles pursue a different goal from the rules on unfair contractual terms (Art. 13) or the rules on making data available to public sector bodies (Art. 14 *et seq*.). Completely different objectives are also pursued by the rules on switching between data processing services and interoperability (Art. 23 *et seq*.; Art. 28 *et seq*.), the rules on international transfer or governmental access to non-personal data (Art. 27) or the rules on smart contracts (Art. 30).

When it comes to the rules on the access rights of users, these different goals lead to complex regulations that partly contradict themselves. For example, one could imagine various case constellations in which the user wants to make his data available to third parties in accordance with Art. 5. Here, the third party could be a data trustee but it could also be a company that needs the data to provide services - possibly competing with services of the data owner. It could even be a start-up that wants to develop new types of services and to which the user wants to make this data available in order to develop these services. Other use cases are conceivable. The Draft Regulation is only partially successful in regulating all these use cases, each with clearly different interests of the parties involved. Coupled with other regulatory complexities, the Draft Regulation contains several ambiguities and contradictions. The DAV therefore proposes - as already argued in Position Paper No. 50/21 when responding to the Public Consultation - to separate the various legislative complexities and to enact individual legislative acts

that can deal more concretely with the respective regulated norm complex and its problems (p. 4). Even then, a horizontal regulation will only be possible if it contains a norm for the general balancing of interests similar to Art. 6 (1) sentence 1 letter f of the GDPR.

Furthermore, the Draft Regulation contains two completely contradictory rules on how to deal with other Regulations: While the right to a database always takes second place to the rights to access data, the regulations on data protection always take precedence. Art. 8 of the EU Charter of Fundamental Rights (CFR) establishes the fundamental right to data protection. However, the rights of the database owners are also protected as a fundamental right, namely under the provisions on the right to property according to Art. 17 CFR. Hence, the differing treatment between the right to a database and the right to data protection is not justifiable. The Draft Regulation establishes rights to data access. However, the current regulations will prevent the disclosure of personal data to persons other than the data subject. This means that the rights to data access will not be practicable: The data subject already has the envisaged rights of access under Article 15 GDPR. Under this provision, he already has a right not only to information about the data stored about him, but also a right to the transmission of data copies (Article 15 (3) GDPR). Anyone who is not a data subject will not receive any personal data of third parties under the Draft Regulation either. This would only be different if there were access rights also with regard to personal data of third parties, in other words, if claims under the Draft Regulation would create a legal obligation according to Art. 6 (1) sentence 1 lit. c GDPR. However, when creating a norm for this purpose, it is necessary to balance the rights and interests of the fundamental right to data protection with the rights to a database. This new norm should be phrased in a manner comparable to Art. 6 (1) sentence 1 lit. c GDPR. The inclusion of one or several such provisions (depending on the complexity of norms) regarding the balancing of interests is urgently needed.

2. Basic regulatory approaches

When it comes to large platforms, there are too few competitive European providers. This can be seen when considering the difficulties in implementing the Schrems II ruling (C-311/18, 16 July 2020). Due to network effects, consumers and entrepreneurs do not have sufficient choice when choosing a platform provider and need to accept data

processing processes that are in breach of the GDPR.[1] The lack of alternatives to the central platforms (especially in the area of cloud infrastructures) seems so great that even court rulings,[2] more consistent enforcement by the EU data protection authorities[3] and the threatening potential of very successful data protection activists can only slowly initiate a turnaround.

The plans of the Commission[4] to break the lock-in effects regarding large platforms and to allow both individuals and other market participants to take part in the economisation of data are as old as the GDPR. Data portability and interoperability were recognised as prerequisites early on. In this respect, the objective of the Data Act to create data access rights is to be welcomed.

The material scope of the Draft Regulation explicitly refers to data-intensive use cases. In particular, these are physical products that collect or generate data about their performance, use or environment through corresponding components as well as transmitting such data via a publicly accessible electronic communication service. Recital (14) refers to this as the 'Internet of Things' ('IoT'). Such IoT products may include connected vehicles, household appliances and other consumer products, as well as medical devices and agricultural or industrial machinery. It is typical for IoT products that they are operated by different users and that data of different persons is being processed. It may not be clear to users, manufacturers or the 'data holder' who exactly the data subject is. Where consent is required, this would have to be obtained from third parties. In other words, the consent of a data subject does not apply to the data of third parties.

[1] Compare ruling of the Federal Supreme Court of Germany (BGH), KVR 69/19 – Facebook, 23 June 2020.
[2] OVG Schleswig, Judgement of 25 November 2021 - 4 LB 20/13; LG München, Judgement of 20 January 2022, 3 O 17493/20.
[3] About Google Analytics: decision of the Austrian data protection authority of 22 December 2021 - GZ: D155.027 2021-0.586.257; press release of CNIL of 10 February 2022; notification of the Dutch data protection authority of 13 January 2022.
[4] Communication of the Commission 'Building a European Data Economy', COM (2017) 9 final of 10 January 2017.

The following fundamental problems regularly arise in such data markets:

(1) In many cases, personal-data are not easy to separate from non-personal data. The anonymisation of data is often not possible without considerable loss of quality as well as usability. This is especially relevant for the training data of artificial intelligence (AI) applications, which is an important use case of the Data Act.

(2) The GDPR establishes the principle of data minimisation for the processing of personal data (Art. 5 (1) (c), Art. 25 GDPR). This principle is now extended to non-personal data in the Draft Regulation, which is a conflict of objectives with regards to data quality.

(3) Data pools are another use case for the Data Act. When personal data (which is often inseparable from non-personal data) is present in such data pools, data subjects have to be sufficiently informed about the collection and provision of their personal data. The Data Act is intended to apply to data that is provided by users but also to data that is generated by the use of products. This applies, amongst others, to diagnostic data, *cf*. Recital (17) of the Data Act. Currently, there is a lack of transparent information, for example regarding the click section of websites and apps (instead of excessive or too general data protection declarations). What is also lacking is sufficient choice between products with minimal data processing, products that process data in relationship with few individual marketing purposes and products with comprehensive data processing and profiling. In light of increasingly complex profiling and limited digital competence of many consumers, this is a challenge for companies. At the same time, this is a prerequisite for a functioning data market.

(4) If transparent information is not provided, consent is all the more impossible as a legal basis for processing data. Even with transparent information, both consent (due to the ‘prohibition of tying’, Art. 7(4) GDPR) and contract performance (Art. 6(1) sentence 1 (b) GDPR) remain currently questionable as a legal basis (see also the ongoing case C-446/21, Schrems - III). In cases where data of third

parties (for example, in the case of IoT devices or vehicles) are processed and cannot be separated, both consent and contract performance cannot be used as a legal basis. Therefore, a statutory legal basis is required. The Draft intends to leave the obligations under the GDPR unaffected and in some cases even supplements them with additional obligations. Access to data or making data available is to be governed by the Data Act. However, the Draft does not aim to create any legal basis (in terms of data protection) for data processing activities. In IoT-cases where user and data subject are not identical, the 'data holder' may only provide personal data when there is a legal basis under Art. 6 or 9 of the GDPR (Art. 4(5) of the Draft). In contrast, non-personal data may only be used by the data holder himself when there is a contractual agreement with the user (Art. 4(6) of the Draft).

The Draft aims to create a viable regulatory model for data access by establishing fair contractual regulations between a **triangle** of participants (data holder – user – data recipient/third party). However, in many cases - such as smart homes, connected cars or virtual assistants – this triangle is likely to become a **square** (as Art. 4(5) of the Draft suggests). In cases where the user is not the data subject within the meaning of the GDPR, the data subject will be added as a fourth party in addition to the user. Whether a contractual arrangement exists between the data subject and the (B2B-) user or between the data subject and the data holder is unclear. It also remains unclear whether such a contractual arrangement might actually establish a legal basis (see above (4)). This is even more problematic when one adds personal data of guests or passengers of users. Therefore, a bilateral contract between the data holder and user is not a sufficient legal basis in regard to **these data of the 'fourth party'**. This mixture of personal and non-personal data is not the only case that needs to be considered in the regulatory approach of the Draft. Data files of users which (inseparably) show a reference to a data subject other than the user, as well as data with multiple references would also have to be included. This requires the establishment of a new legal basis as well.

The regulatory approach of Draft will not be achieved as long as:

- the Draft aims at being only complementary to the GDPR,
- the GDPR only deals with individual data subjects and does not create a clear regulatory scope for data processors,
- the data protection authorities continue to restrict scope and purposes of processing that can be based on a legitimate interest under Article 6(1)(f) of the GDPR, and
- the ‘Schrems II’ issue remains, which is often unavoidable in cases with international providers; this remains insoluble to practice in many cases.

To achieve a successful regulatory approach in the Data Act and to achieve a competitive European data economy, it is crucial to create additional legal bases. At the same time, the mentioned legal uncertainties must be eliminated. If it is impossible to create these prerequisites in the Data Act, it must be done by modernising the GDPR. The Data Act can only be successful if the establishment of a new legal basis takes place simultaneously and does not remain unclear. To achieve this, the fact that the Draft states that the GDPR and Directive 2002/58/EC should remain unaffected by the Data Act is not sufficient. Otherwise, it is very likely that ‘data holders’ will not be allowed to make data accessible in many cases – even if they wanted to, due to conflicting obligations under the GDPR.

3. Relationship of the Draft to data protection rules and principles

Recital (7) seeks to clarify that the provisions of the Draft must not be applied or interpreted in such a way as to compromise or eliminate data protection, privacy and the confidentiality of communications. The provisions of the GDPR and Directive 2002/58/EC should therefore retain maximum validity. The national implementations of Directive 2002/58/EC and the future EU e-Privacy Regulation should also remain unaffected. This affects the German TTDSG (Data Protection Act for Telecommunication and Telemedia), *cf*. Recital (32) Data Act. Similar to the DC-Directive 2019/770/EU, the Data Act intends to leave the data protection provisions unaffected. However, unlike the DC-Directive, the Data Act contains various provisions that do affect the GDPR.

Recital (7) recognises that in practice a mixture of personal and non-personal data is common. Accordingly, Recital (7) concludes that data protection principles should also apply to data sets containing a mixture of personal and non-personal data.

Recital (8) mentions essential principles of the GDPR such as data minimisation and data protection through technological design and through data protection-friendly default settings, if data processing entails significant risks for the fundamental rights of the individual. State-of-the-art technical and organisational measures as well as encryption are also explicitly mentioned. However, it is not clear in the Recital to what extent these requirements relate exclusively to personal data. The Data Act leaves open how data minimisation is compatible with AI applications (even if it is only weak AI in form of intelligent algorithms), which is an unresolved fundamental problem.

Recital (8) specifies that data (personal and non-personal?) should be analysed by algorithms 'without the transmission between parties or unnecessary copying of the raw or structured data themselves'. This approach is to be welcomed in principle. However, its exact meaning and scope remain unclear, as well as a specific use case for this scenario. The wording suggests that processing by algorithms is considered permissible, however, the relationship to data protection rules, *i.e.*, whether processing exists within the meaning of Art. 4 (2) GDPR, is not apparent. Either Recital (8) only deals with non-personal data and extends typical principles of the GDPR to it. Or the example on algorithms also concerns personal data, but then it reads like the permission that is explicitly not intended according to Recital 24.

4. Unclear definition of the 'data holder'

In the Draft, the **'data holder'** is the **central addressee of obligations**. He is obliged to 'share' data with third parties in accordance with the provisions of the Draft. In this way, the monopolisation of 'data silos' can be counteracted in order to promote **innovation and competition** (*cf*. for example Mayer/Schönberger, Das Digital, 2017). This general approach of the Draft is to be welcomed.

If it is primarily about obliging a certain 'data holder' to 'share' data, it is necessary that **the definition of the norm addressees is as precise as possible**. It would not be desirable that what applies to 'data silos' in markets with monopolistic tendencies is extended to data holdings of medium-sized companies or to emerging start-ups. This

holds particularly true if one does not want to create **a 'one size fits all'** solution that impedes smaller companies in competition with 'big players'. This would weaken new and innovative companies instead of strengthening them.

Art. 2 (6) of the Draft defines the term 'data holder' *as 'a legal or natural person who has the right or obligation, in accordance with this Regulation, applicable Union law or national legislation implementing Union law, or in the case of non-personal data and through control of the technical design of the product and related services, the ability, to make available certain data'.*

There might be an editorial error in the German translation of the Draft (the word '*und*' after '*bzw. im Falle nicht personenbezogener Daten*' should be deleted). The English version of the definition is clearer in that regard, as a data holder should be somebody that is authorised or obliged to make data accessible.

This definition makes no reference to the objectives pursued by the Draft. It is not apparent why the definition neither differentiates between **companies of different sizes** nor is linked to **criteria of 'data power'**. Without such 'data power', it remains unclear why there should be a need for regulation of the respective companies at all.

Art. 2(6) of the Draft also has a circular tendency, as it is linked to **'obligations'** of the 'data holder' with regards to data, although it is actually a matter of the Draft to impose such obligations on the 'data holders' in the first place. Only in the case of non-personal data does it depend (solely?) on the 'data holder' being technically capable of making the data available. In addition, and unrelated to this, there is a link to 'rights', without it being clear whether this is to be understood in terms of ownership, copyright or otherwise. Furthermore, it is not atypical for several actors to have different rights to data files. This **conflict of rights** arising as a result needs to be resolved. What the Draft leaves open is its **relationship with the responsibility under data protection law.** Similarly, the yardstick regarding the actual circumstances ('the ability') which the Draft refers to remains unclear. This concerns both the circumstances alone as well as their interaction with the other criteria included in the definition.

5. Ambiguities regarding responsibility under data protection law

Recital (24) explains that the ‘data holder’ shall be obliged to make data available under certain circumstances. Further, Recital (24) assumes that the ‘data holder’ – in regard to the processing of personal data – is also the data controller within the meaning of Art. 4 (7) GDPR. What remains unclear is whether this means that only data holders (and not processors) may make data accessible to third parties and are hence considered ‘data holders’ within the meaning of the Data Act.

According to Art. 2 (6) and Recital (24) of the Draft, it is difficult to determine who can be a ‘data holder’. This makes it complicated for companies to clarify whether and when they fall within the scope of the Data Act. It is understandable that the data holder´s obligation to disclose data pursuant to the Draft leads to him being responsible under data protection law. However, the obligation itself cannot be derived from that circular definition. Therefore, according to the definition of the ‘data holder’, the Data Act only obliges a person that is already considered a ‘data controller’ independently of the Data Act. If the person is not a data controller, no data holder-obligations apply under the Data Act.

Furthermore, the assessment of whether a data processor is a data holder, a joint data holder (possibly jointly with the manufacturer or with the B2B customer) or a processor is determined by the GDPR or, if applicable, by Member State law pursuant to Art. 4 (7) GDPR (‘where the purposes and means of such processing are determined by Union or Member State law...’). At the moment, the Draft Data Act is not a regulation that regulates the purposes and means of processing in a sufficiently specific manner.

The obligations of the data holder under Articles 4-6 of the Draft are limited to data ‘generated by the use of a product or related service’, which may include a virtual assistant. The definition of ‘related service’ in Art. 2 (3) of the Draft is modelled according to the definition of ‘goods with digital elements’ in Art. 2 (5) (b) of the Sale of Goods Directive 2019/771/EU.

IoT applications (*e.g*. in the area of smart homes) or solutions for networking cars and commercial vehicles (e.g. with manufacturers, insurers and workshops, etc.) are often based on central platforms in the back-end. Those platforms are hosted and operated by a platform operator together with the corresponding application software and databases. In some cases, the data that the user provides and that is generated when

using the product might converge there. Sensor data and image data may be converted into data formats that can be further analysed or read out and stored as structured data that can be further processed.

In practice, especially, platform operators or SaaS providers often (want to) act as processors for their customers, but at the same time they use the data (or at least diagnostic and telemetry data) for their own purposes (*i.e.* not as processors). In this respect, the data holder should specifically undertake the processing activity of making the data available in accordance with the Data Act, even though he predominantly acts as a processor. The wording is not clear at this point.

6. Unclear relationship between producer and 'data holder'

Art. 3 (1) of the Draft obliges the manufacturer to make data 'directly accessible to the user'. The exact meaning of 'directly applicable' remains unclear, especially in constellations of 'shared use':

- What exactly are the criteria for 'directly accessible' data? Is this based on an **'average user'** without special technical skills?
- **'Shared use'** is regulated in Recital 20. Separate user accounts are proposed there. But 'shared use' can also take place simultaneously. For example, in the case of a vehicle, the owner has an interest in the vehicle data, even if this data is generated during the journeys of a third party. Who should then be authorised to access the data? Both? How can this be harmonised with the GDPR?

What remains open are the legal consequences for the manufacturer. For technical reasons, manufacturers might not be able to make data 'directly accessible'. There might also be other reasons why a manufacturer wants to put a product on the market that does not give the user the possibility of 'directly accessible data'. In this scenario, **Art. 4 (1) of the Draft**, for no apparent reason, does not oblige the manufacturer to ensure 'directly accessible data', but rather the 'data holder' who must provide the user with the generated data. This will not always be possible for the 'data holder' without **technical support from the manufacturer**. However, there is no provision establishing an obligation of the manufacturer towards the 'data owner' that corresponds to the

obligation of the ‘data holder’ according to Art. 4 (1) of the Draft, enabling the latter to provide the user with direct access to the data.

It also seems inconsistent that Art. 3 (1) of the Draft obliges the manufacturer to provide ‘directly accessible data’ without distinguishing between personal data and non-personal data. At the same time, **Art. 4 (5) of the Draft** obliges the ‘data holder’ to exclude access to personal data if there is no legal basis for such access under Art. 6 or Art. 9 GDPR. Here, too, the question arises as to how such a differentiation should be possible for the ‘data holder’ without the help of the manufacturer. In any case, there is no provision obliging the manufacturer to provide assistance.

According to **Art. 4 (6) sentence 1 of the Draft**, the ‘data holder’ may only use data generated during the use of the product for his own purposes if he is contractually permitted to do so. A corresponding restriction of data use for the manufacturer is missing, without any apparent reason for the different treatment.

In **Art. 3 (2) of the Draft**, sellers, lessors and leasing companies are obliged to **inform the user about data processing procedures**. In many cases, sellers, lessors and leasing companies will not be able to fulfil these obligations without the support of the manufacturer. Nevertheless, there are no corresponding obligations of the manufacturer towards the ‘data holder’ in the Draft. Particularly problematic is the obligation to determine the ‘data holder’ under Art. 3 (2) (e) of the Draft. In view of the vague definition of the ‘data holder’ in Art. 2 (6), this cannot be easily fulfilled. The relationship between the seller or lessor mentioned in Art. 3 (2) of the Draft and the ‘data holder’ also remains unclear.

Art. 4 (6) sentence 2 of the Draft prohibits the ‘data holder’ from using data generated during the use of the product with the aim of gaining knowledge about the user which could affect his or her position in the market. It remains unclear whether this prohibition is dispositive, *i.e.*, whether the user can waive the protection justified by the prohibition. (This would be a regulatory approach of **Art. 5 (5) which has been formulated differently** and deals with the market position of the third party that obtains access to the generated data at the request of the user).

Almost all obligations in Chapter II are directed at ‘data holders’, but not at manufacturers. **The exemption for small businesses** in **Art. 7 (1) of the Draft** is convincing, *cf*. also Recital 37. However, the wording leaves open whether the exemption also applies to **(larger) ‘data holders’** who use **products manufactured by small businesses**. If Art. 7 (1) of the Draft is indeed to be understood in this way, it would be doubtful whether such an exemption for larger ‘data holders’ can be reconciled with the goal of counteracting the emergence and consolidation of ‘data power’.

Article 7 (2) of the Draft extends the provisions of Chapter II to ‘virtual assistants’. It is not clear what exact **use cases** are to be covered by this.

7. The rights of data subjects, profiling and some minor issues regarding the legal basis under data protection law

Recitals (23) and (24) address the practical problem that information duties, enquiries, copying and data portability claims of data subjects can arise from the GDPR as well as from the Data Act. One example is Art. 3 of the Draft. Paragraph 1 regulates concrete design requirements for the product regarding direct user access to personal data. With regards to personal data, this is a concretization of Article 25 of the GDPR. It is questionable whether the design requirement of direct accessibility is appropriate in all applications (such as onboard modules of vehicles or medical devices); however, the obligation is restricted with the requirement of being ‘relevant and appropriate’, which creates room for consideration and balancing of interests.

It is not entirely clear who has to fulfil the additional information obligations under Art. 3 (2) of the Draft. The data holder is only mentioned as a duty addressee from Art. 3 (2) (e) onwards. It is possible that the information duty is directed at the manufacturer (see Art. 3 (2) (d)). However, the manufacturer can hardly fulfil Art. 3 (2) (e) to (g). In Art. 3 (2) (e), the German translation misleadingly refers to the ‘address of the place’, which probably means the entire postal address. Regarding personal data, the obligations of Art. 3 (2) supplement the information obligations from Arts. 13 and 14GDPR. When the user is a data subject, Art. 3 (2) (a) of the Draft means that, in deviation from Art. 13 GDPR, the types of data must also be indicated if the data are

collected from the data subject. In practice, however, this should already be done frequently.

Art. 6 (2) (c) of the Draft poses greater difficulties. It concerns a third party/data recipient who receives personal data pursuant to an agreement with the user - ‘subject to the rights of the data subject’ according to the GDPR (Art. 6 (1) of the Draft). Art. 22 (1) GDPR prohibits profiling if it ‘produces legal effects concerning him or her or similarly significantly affects him or her’. Article 6 (2) (c) of the Draft generally prohibits profiling in the sense of the GDPR. Yet, it would be questionable anyway on which legal basis the third party would be able to rely on regarding profiling. However, Art. 6 (2) (c) of the Draft makes an exception to this prohibition insofar as the profiling is necessary to fulfil a service expressly requested by the user. Here, it should be clarified that this is also a legal permission in the sense of data protection law. Otherwise, a clarification regarding Art. 22 (1) GDPR would be necessary for cases involving personal data of persons other than the user, and for cases in which an effect expressly desired by the user is to occur due to profiling, but which is a ‘legal effect’ within the meaning of Art. 22 (1) GDPR.

Insofar as the user requests to receive personal IoT data relating to him or her from the ‘data holder’, the regulations on the data sharing obligation supplement his or her right to data portability under Art. 20 of the GDPR (see Art. 1 (3) of the Draft). If the user is a company and thus not a ‘data subject’ within the meaning of the GDPR, he can become a ‘data holder’ himself by receiving the IoT data (see Recital 30) and would then in turn be obliged to share data with his users.

According to Art. 23 *et seq*. of the Draft, providers must ensure that customers can switch to another service provider with a comparable service and transfer the corresponding data. While Art. 20 (1) of the GDPR regulates the right to data portability for personal data provided by a data subject himself, the same shall apply to all data within the scope of the Data Act. A user may request to ‘share’ data with certain third parties (‘data sharing’), *e.g*. to provide such a third party with a copy of the data. For personal data, this can be interpreted as a supplement to the right to data portability under Article 20 (1) of the GDPR.

In Recital (20), the Draft addresses the fact that there may be different people involved when it comes to owners or tenants and that data may be collected about different

persons. It is also mentioned that there are typically different user accounts. However, this does not solve the problem of the legal basis for data protection. In addition, the Association of German Data Protection Authorities (Conference of the Independent Data Protection Authorities of the Federation and the Länder, DSK) requires in a Resolution[5] that continuous user accounts in online commerce may only be maintained with prior consent and that consent is only effective if the user is alternatively given the opportunity to carry out the transaction as a 'guest' without a user account. The fact that the user account is maintained for the purpose of executing a tele-media usage contract with the user (Art. 6 (1) (b) GDPR) does not seem possible from the perspective of the data protection authorities. A legal basis that is established due to a contract with the user is increasingly being pushed back in data protection law.

Perhaps PIMS (Privacy Information Management Systems) can be helpful in the future. The expected legal regulation of the German Federal Government for 'recognized services for consent management, end user settings' (Section 26 (2) TTDSG) should be considered in this context.

If the processing of personal data is based on consent (possibly also from persons who are not users) or on legitimate interest (Art. 6 (1) sentence 1 (f) GDPR), revocation of consent or objection according to Art. 21 GDPR with future effect may lead to unlawful processing. The Draft does not regulate what effect this has on data already provided to users or to third parties/data recipients. Who in the triangle of data owner - user - third party/recipient has to fulfil which tasks in this respect and must bear which costs? Legal clarification would also be desirable in this respect, for example if data was used to train AI and must have been documented. Art. 17 (3) (b) and (e) of the GDPR provide exceptions to the obligation to delete data. But clarifications that especially concer the application of the Data Act would be necessary. The need for clarification here is likely to be even greater than in the case of assertion of revocation or objection in cases of 'payment with data' according to § 327 (q) German Civil Code (BGB).

8. Problematic transfer of regulatory models under data protection law to non-personal data

[5] 'Datenschutzkonformer Online-Handel mittels Gastzugang' (https://datenschutzkonferenzonline.de/media/dskb/20222604_beschluss_datenminimierung_onlinehandel.pdf), dated 26 April 2022.

The Draft often introduces **legal ideas and regulatory methods** that are known from **data protection law**. For example, **Article 6 (1) of the Draft** is characterised by the principle of earmarking.

The **principle of earmarking** has constitutional status as far as personal data is concerned, according to **Art. 8 (2) sentence 1 EU Charta of Fundamental Rights (CFR)**. This principle should not be extended to data for which there is no comparable protection of fundamental rights without necessity, as this could **dilute the principles of data protection law**. The more one applies data protection rules to non-personal data, the more **diffuse** will the **idea of protection** pursued by these rules become.

Art. 11 (2) of the Draft regulates the use of **public law enforcement** (by authorities, *cf*. Art. 31 of the Draft) to **enforce private law obligations** to delete data. Unless this would concern personal data that are protected under Art. 8 CFR, this is not understandable. If the existing legal bases were not sufficient (in German law *e.g*. § 1004 BGB), claims under private law for injunctive relief or deletion would definitely be sufficient.

The same applies to **Article 27 of the Draft**. Art. 27 extends Art. 44 *et seq.* GDPR to non-personal data. Although this happens in a slimmed-down way, it **makes international data traffic more difficult**, without this being justified by Art. 8 CFR. The reasons for these restrictions on the export of non-personal data to a third country remain open.

Articles 32 and 33 of the Draft contain provisions on the administrative enforcement of the Data Act, whereby Article 32 of the Draft is obviously based on **Articles 77 and 78 of the GDPR**. It therefore deals with **administrative procedural law** (Art. 32 of the Draft) and **substantive criminal law** (Art. 33 of the Draft). These harmonising European regulations established by Art 77, 78 and 83 GDPR are legitimate regarding the protection of the fundamental rights under Art. 8 CFR. However, it is not apparent why such harmonised foundations for procedural rights and fines are necessary within the Data Act, which is not primarily concerned with the protection of fundamental rights.

9. Excessive restrictions on freedom of contract

Freedom of contract is restricted by numerous provisions of the Draft, without a **clear frame** being apparent to guide these restrictions. For example, it is not clear why the 'data holder' is not only obliged to make the data available to third parties without delay and free of charge (as set out in **Art. 5 (1)**), but is also obliged to comply with certain conditions for contracts on making data available according to **Art. 8 (1) of the Draft**.

Similarly, it is confusing when **Art. 5 (1) of the Draft** states that the user should determine who the 'data recipient' is, while at the same time **Art. 8 (3) and (4)** contain requirements for the 'data holder' regarding the selection of the 'data recipient' as well as regarding the drafting of the contract with the 'data recipient'.

10. Protection of trade secrets

Data within the meaning of the Data Act may in some cases **qualify as a trade secret** according to the Trade Secrets Directive (**Directive (EU) 2016/943**). The Draft of the Data Act states in various places that trade secret protection must be taken into account when exchange of data is planned – at least between private parties (*e.g.* in Art. 4 (3) or Art. 5 (3)).

However, the conception of a general right to access data as perceived by the Data Act is in conflict with the Trade Secrets Directive. **According to the Trade Secrets Directive, access to trade secrets is to be restricted and controlled**. According to the Data Act, one can gain a right of access to all data that falls under the scope of application of the Data Act. Besides the user, this also applies to an unrestricted circle of third parties – derived from the users. This brings with it the risk that the corresponding data is classified as easily accessible. Hence, due to the new regulations of the Data Act this data might lose its secrecy status granted under the Trade Secrets Directive. Clarifications are necessary that exclude such a contradiction. Besides this, the factual risk to lose control and thus lose the secrecy status should not be underestimated, especially since the circle of data recipients cannot easily be restricted.

Due to the triangle 'data holder – user – third party', data holders might not be able to sufficiently secure the protection of their trade secrets by way of contract. Firstly, the 'data holder' as defined in Art. 2 (6) of the Draft does not necessarily have to be identical with the owner of a trade secret as defined in Art. 2 (2) Trade Secrets Directive. The 'control' required in each case is defined differently in the two legal acts.

The Data Act does not regulate how a trade secret owner who is not a data holder at the same time is to be included in data exchanges. This leads to a lack of protection in such cases. Even in cases where data holder and trade secret owner are identical, it is not the data holder but the user who (1) selects the third party to whom the data is to be disclosed, (2) agrees with the third party on the purposes for which the data is to be used (Art. 6 (1)) and (3) determines whether exclusivity is permissible (Art. 8 (4)). Currently, data use by third parties is only to be excluded for the development of a product 'that competes with the product from which the data originate'; the same applies to disclosure to other third parties (Art. 4 (4) or Art. 6 (2) (e)). This severely restricts the ability of trade secret owners who are not among the micro or small enterprises privileged under Article 7 to further develop their own products and services. They must fear that third parties - *e.g*. larger and/or more financially powerful ones - will beat them to such developments with their own data. Moreover, this risk does not only exist with regard to third parties, but can also arise with users themselves, for example if they are legal entities of a certain size. Therefore, the aforementioned restriction of data use by third parties should also be extended to the users themselves. Chapter V, which regulates data access by public bodies, should be supplemented with regulations on the protection of trade secrets. Finally, it is necessary to clarify that Article 11 and Recitals 8 and 21 do not impose more stringent obligations on data holders with regard to secrecy measures in order for them to be considered 'reasonable' within the meaning of the Trade Secrets Directive.

11. Relationship of the Data Act with Competition Law

The Data Acts implements new EU rules on the use of and access to data generated in the EU across all sectors of the economy. It aims to ensure fairness in the digital environment, promote a competitive data market, open up opportunities for data-driven innovation and make data more accessible to all.

The Data Act includes four main types of measures/regulations:

(1) measures to allow users of connected devices to access the data they generate and to share this data with third parties to provide the aftermarket or other data-driven innovative services with the data (*e.g.* **Article 5**);

(2) measures to rebalance the bargaining position of SMEs by preventing the abuse of contractual imbalances in data sharing contracts. Measures include protection against unfair contractual terms imposed by a party with a much stronger bargaining position (e.g. **Article 13**);
(3) the ability for public sector bodies to access and use data held by the private sector in exceptional circumstances, in particular in public emergencies (e.g. **Article 14**);
(4) new rules allowing customers to effectively switch between different cloud data processing service providers and providing safeguards against unlawful data transfers (e.g. **Article 23**).

The main competition law provisions are contained in **Articles 101 and 102 of the Treaty on the Functioning of the EU (TFEU)**. Article 101 TFEU prohibits all agreements between undertakings, decisions by associations of undertakings and concerted practices which may affect trade between Member States and which have as their object or effect the prevention, restriction or distortion of competition within the internal market. Article 102 TFEU prohibits undertakings of a dominant position within the internal market or in a substantial part of it from abusing that position.

At first glance, the competition law provisions and the new provisions of the Data Act regulate two different areas and should therefore not interfere with each other. However, if one looks closely at the content of the new provisions, one realises that there may be certain conflicts between the provisions, especially with regard to the **exchange of information** between competitors.

As mentioned above, the first conflict between the Data Act and the competition law provisions could arise in the context of the obligation for data holders to share product-generated data with end-users as well as with third parties. Even though Recital 88 of the draft provides that the proposal ‘should not affect the application of the rules of competition, and in particular Articles 101 and 102 of the Treaty’, typical risks of competition law could arise from the application of the Data Act. Indeed, **Art. 5 of the Draft** includes an obligation for data holders to make available the data generated by the use of a product or related service to a third party, without undue delay, free of charge to the user, of the same quality as is available to the data holder and, where

applicable, continuously and in real-time, upon being requested by a user. This poses a risk to competition law, since the exchange of sensitive information - especially between competitors - can be considered a serious breach of competition law.

The Draft does not distinguish between the type of data involved. Therefore, the exchange could involve – among other types of information – commercially sensitive information about actual or potential competitors. This goes beyond the exchange of data that is valuable for use by companies. As part of the revision of the new horizontal block of exemption regulations and the new horizontal guidelines, the Commission published a Draft containing revised horizontal guidelines in March 2022. These include a more detailed chapter on the impact of information sharing. According to this, the main competition law risks arising from the exchange of data pools, as by the means of the Data Act, are the result of **collusion** and **anti-competitive foreclosure**.

On the one hand, **collusion** may occur because the exchange of information increases transparency between competitors on the market. Therefore, this facilitates coordination of competitive behaviour of undertakings, especially where data is considered sufficiently ‘commercially sensitive’. This may lead to restrictions of competition.

On the other hand, **anti-competitive foreclosure** may occur in cases where the exchange of commercially sensitive information leads to situations where competitors that do not participate in the exchange suffer a significant competitive disadvantage compared to the undertakings affected by the exchange. The guidelines do not specifically address data sharing based on obligations arising from EU legal frameworks such as the Data Act. However, they do address how data sharing initiatives can lead to anti-competitive foreclosure if competitors are denied access to data or are only granted access on less favourable terms. In order to comply with the rules of competition law and at the same time fulfil the obligation under **Art. 5 of the Data Act**, data holders would have to provide the data under conditions that are not less favourable than the conditions under which the data holders had access to the data.

The future **Digital Markets Act (DMA)** imposes similar obligations on ‘gatekeepers’ in relation to data access and data portability as the Draft proposes. However, as a main difference, the Data Act explicitly excludes ‘gatekeepers’ from benefiting from data access rights provided for in the Draft. The reason for this exclusion is mainly due to these entities’ exceeding capacity to obtain data. Hence, including them into the scope

of the Data Act would not serve its objectives. The provisions of the DMA could be in conflict with competition law, where competition law regulations affect the exchange of commercially sensitive information. To offset these potential risks, the exclusion of gatekeepers from data access rights could serve as a safeguard against potential breaches of competition law. In addition, **Art. 6 of the Draft** contains additional safeguards to avoid competition law risks. This is done by imposing obligations on third parties that receive data at the request of the user. The use of smart contracts for the exchange of data that meet the requirements of **Art. 30 of the Draft** would be an excellent tool for the common use of data, while at the same time reducing risks arising from competition law due to the exchange of commercially sensitive information.

However, despite the safeguards provided for in **Art. 6**, the current version of the Draft carries a potential risk of competition law infringements. These arise in the form of unlawful exchange of commercially sensitive information. The Draft contains some legal uncertainty for data holders and third parties when exchanging data at the request of the user. Therefore, one should aim for clarification on the relationship between the obligations arising from the EU digital legal framework (e.g. Data Act) and the prohibition of sharing of commercially sensitive information between competitors. The Draft was open for feedback from stakeholders until 13 May 2022. Currently, the Commission is assessing the comments received. We will see whether the Commission has taken this issue into account or whether uncertainty will remain regarding the application of the Data Act.

12. General exclusion of the applicability of database law

Article 35 provides that the *sui generis* right granted by Art. 7 of the Database Directive 96/9/EC shall not apply to databases obtained or created through the use of a product or related service falling within the scope of the Data Act. This is to avoid obstructing the users' right to access and use such data under Art. 4 or to disclose such data to third parties. One can consider that it is only possible to achieve the objectives of the Data Act with certain restrictions of the rights to database However, even this consideration does not justify the general exclusion of this right. After all, even databases containing a collection of machine-generated data created through the use of products or related services may require a ‘substantial investment’ within the meaning of Section 87a (1) German Copyright Act (Urheberrechtsgesetz, UrhG). This

‘substantial investment’ would be without any legal protection in the current overall denial of applicability of database law. However, it has not yet been decided by the highest courts that machine-generated data do not enjoy database protection. There are, indeed, weighty reasons for such protection – these are also discussed in length in the literature regarding the considerable investment required for this. Since the vast majority of data will be generated and systematised automatically in near future, database law would largely come to nothing if this exclusion were maintained. Therefore, the data holder should be given the opportunity to prove that a substantial investment was required for the acquisition, verification or presentation of the data in a machine-generated databank. If access to such data is considered necessary in these cases, this could be provided for against payment of an appropriate fee.

13. Duty of making data available to public sector bodies (Chapter V)

Chapter V of the Draft deals with the obligation of private parties to make data they hold available to public sector bodies when there is no such obligation otherwise imposed by law. According to Art. 14 and 15, this should be possible in cases of exceptional need. The Draft provides for three of those exceptional needed cases:

The first case, set out in Art. 15 (a) of the proposal, is unproblematic. In cases where public sector bodies need the data to combat a public emergency, data has to be disclosed by the data holders. This seems understandable and is justified. This is even more so since such a request by public sector bodies must be proportionate in terms of granularity, scope and frequency of the data release. It must also consider the legitimate interests of the data holder that must make the data available, his or her costs and potential trade secrets (Art. 17 (2) (b) and (c)). According to Art. 15 (b), data must also be made available where it is necessary to prevent a public emergency or to assist the recovery from a public emergency, where the data request is limited in time and scope. According to Recital 58, this only concerns the prevention of an imminent public emergency and the assistance regarding the recovery from a public emergency, in circumstances that are reasonably proximate to the public emergency in question. The additional requirements of Art. 17 (2) (b) and (c) apply as well. It is justified that such requests to make data available must be reasonable. It would be impossible to regulate specific requirements for all kinds of emergencies in special laws. However, the requirement of temporal proximity as a restriction of the obligation to make data

available, as contained in Recital 58, should also be included in the text of Art. 15 (b) itself.

Overall, the obligation to make private data available in public emergency situations, seems legitimate. Nevertheless, an additional provision should be included that ensures the protection of data that are subject to professional secrecy. At the moment, no provisions that protect professional secrecy can be found in the Draft. Even in public emergency situations, professional secrecy must be protected to the greatest extent possible.

The third case is fundamentally different (Art. 15 (c) of the Draft). Here, data can be requested where the lack of available data prevents the public sector body or Union institution, agency or body from fulfilling a specific task in the public interest that has been explicitly provided by law. At the same time, they must have been unable to obtain such data by alternative means, including by purchasing the data on the market at market rates or by relying on existing obligations to make data available, and the adoption of new legislative measures cannot ensure the timely availability of the data. Alternatively, obtaining the data in line with the procedure laid down in this Chapter would substantively reduce the administrative burden for data holders or other enterprises. As a result, a public sector body can demand to make data available within the scope of its duties in cases where the data is not traded on the market and no special law regulates cases of disclosure. This has the effect that the limits of official requests are very vague, even if the requirements of Art. 17 (2) (b) and (c) must be met. In cases where data is not available on a market, this rule would have the effect that any public task that could be better fulfilled with the data than without would be sufficient to justify a request to make data available. According to Recital 58, such exceptional need may even occur in relation to the timely compilation of official statistics when data is not otherwise available or when the burden on statistical respondents will be considerably reduced. A special law that regulates the conditions and limits of such requests to make data available would not be necessary. It is sufficient that the public sector body needs to access data faster than a law could be enacted. All of this would be possible for public sector bodies even though the respective data may have been collected with considerable expense and of considerable economic value. While trade secrets have to be considered in the context of those requests, the making available of data that contains trade secrets is not *per se* excluded.

According to Art. 17 (2) (d), personal data should not be made available. However, this is not excluded either. In many cases, this will lead to situations where the making available of personal data cannot be avoided in practice. As a result, this norm as well as the request to make data available that are based on the norm, lead to infringements of fundamental rights, including the rights of freedom of enterprise, the protection of property and data protection (Art. 16, 17, 8 CFR). These infringements occur without the definition of the legislator's decision having defined clear conditions in the sense of Art. 52 (1) CFR. Apart from the cases of public emergency described in Art. 15 (a) and (b), this is not justified and is a clear infringement of the CFR. It is particularly alarming that such a request to make data available is possible if the legislator cannot act quickly enough. With the statistical data mentioned in the Recitals, this case is not conceivable. Given the fact that the legislator could enact a law in a few days, this requirement also creates the impression that public sector bodies should be authorised to request to make data available even if the legislator would have wanted to discuss the exact conditions and legal consequences in more detail.

What is also unclear is the significance of the scenario where the data holder would save administrative costs, according to Art. 15 (c). This rule can hardly be used to enable requests to make data available that are already regulated in a more complicated manner. Then this norm would bypass the more specific law or even circumvent the conditions under which data can be made available under other laws. If this is not the intended use case, a request to make data available can hardly reduce the administrative burden, but usually increases it. These concerns exist despite the norm not applying to public sector bodies that carry out activities for the prevention, investigation, detection or prosecution of criminal or administrative offences or the execution of criminal penalties, or for customs or taxation administration (Art. 16 (2)). Even the extensive rules on how to justify a request for data to be made available in Art. 17 (1) of the draft does not change the concern. Neither does the review as laid down in Art. 18 (2). In addition, the right to decline the request in Art. 18 (2) cannot, according to its wording, be used to check whether the conditions for a request for data to be made available according to Art. 15 are met at all. Maybe they could be implicitly reviewed when the conditions of Art. 17 (1) and (2) are checked. However, this should be clarified in Art. 18 (2) of the Draft. Overall, the entire provision of Art. 15 (c) should be dropped.

Further problems arise with the compensation rule contained in Art. 20. The data in question may represent a considerable economic value for the company. In case of a disaster, no compensation should be paid and otherwise only the costs of making the data available (including possible anonymisation) plus a reasonable margin. Debatable is whether the obligation to pay compensation in the cases of Art. 15 (a) of the Draft should be dropped. This provision already leads to compensation for the actual value of the data that has been made available (cf. Art. 17 (1) sentence 2 CFR). This raises doubts as to whether the provision complies with the CFR.

14. Enforcement and Conclusion

Many providers and manufacturers will first have to clarify whether they are considered as ‘data holders’ or manufacturers in the sense of the Draft. The distinction between personal and non-personal data is less important under the current formulation of the Draft, but if legal bases under data protection law are lacking, this is crucial. There will be a mixture of personal data, non-personal data and data of different persons. A separation of this data will hardly be possible (example: environmental sensor data). Anonymisation can help to overcome the lack of a legal basis under data protection law in some areas, but it may not be possible to provide the service desired by the user from a third party/data recipient with anonymous data. Even if the Draft aims at full harmonisation, differing enforcement in the Member States is inevitable, as can also be seen in the different practices of the data protection authorities. It is true that the Member States are to ensure that the authorities involved cooperate in a structured manner in order to avoid duplication. They appoint a coordinating authority. However, it is foreseeable that this will not be sufficient for an effective and pan-European uniform enforcement. The extent to which Member State authorities have sufficient capacity to deal with the foreseeable flood of requests for clarification (in the face of numerous ambiguities) and complaints against (official) data access requests is questionable. The numerous ambiguities will stand in the way of a functioning data market. Currently, the disadvantages for companies due to existing ambiguities outweigh any possible future added value.

15. Miscellaneous

- **Promotion or restriction of ‘data sharing’**: The Draft contains provisions that restrict ‘data sharing’ (e.g. Art. 6), while other provisions are obviously intended to promote ‘data sharing’ (e.g. Art. 13). A decision and clear guidelines are needed here.
- **Arts. 23-27 of the Draft**: On the one hand, the question arises whether there actually is a market failure that justifies the proposed provisions on portability. On the other hand, according to all experience, these provisions are likely to be more burdensome for SMEs than for large companies, which can usually implement standardisation more easily and will also be tempted to impose their own standards on the market.
- **Art. 31 of the Draft**: By designating new ‘competent authorities’, a further element is added to the already existing elements of the European data bureaucracy. It seems preferable to leave the enforcement of the law entirely to the Member States.
- **Art. 34 of the Draft**: It is not clear why the Commission should be tasked with drafting of standard contractual clauses. The **drafting of contracts** is a **matter for the contracting parties** who do not need the support of the Commission.