VI. Right to Share Data with Third Parties (Art. 5-6) and FRAND Obligations for Data Holders When Providing Access (Art. 8-12)

The Data Act aims to break down data silos in order to make them usable for different parties. This is why Art. 5 provides the user with the option to grant a third party access vis-à-vis the data holder. Such an access raises follow-up questions, *inter alia* with respect to the compensation of the data holder, the "how" of granting access and the technical protection measures to be taken. These topics are regulated by Art. 8-12.

1. The Right to Share Data with Third Parties (Art. 5)

Art. 5(1) broadens the user's options. Next to or instead of requesting access according to Art. 4(1), the user has the right to demand access in favour of a third party.

As far as the user's position is concerned, the right resembles Art. 20(2) GDPR.[381] The user may 'port' applicable data sets directly to a third-party entity of their choice. However, the right introduced by Art. 5(1) represents a significant advance over Art. 20 GDPR. The obligations arising between this third party and the data holder are governed in detail through a variety of rules in Art. 6 (and, for data recipients, Art. 8 and 9).[382] At the same time, rec. 25 underlines that the Data Act does not bar voluntary data sharing arrangements emanating from a data holder. This means that in contrast to Art. 20 GDPR, often four or more entities (e.g., data holders other than the party selling or leasing a connected product to the user) will legitimately participate in the sharing of readily available data.[383] Due to multiple actors being involved, the right has also been likened to the transit of goods sold to the "end user" within a complex supply chain.[384]

381 Hennemann, M. / Steinrötter, B., *NJW* 2024, 1 (3).
382 Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 28 n. 70.
383 Schweitzer, H. / Metzger, A., *ZEuP* 2023, 42 (51).
384 Schmidt-Kessel, M., *MMR-Beil.* 2024, 75 (75).

The right granted in Art. 5(1) faces much of the same criticisms as the access right pursuant to Art. 4(1), not least because it is not an independent right of the third party, but is dependent on the user's exercise (and discretion)[385] and, as a result, equally relies on the much-debated premise of user-initiated data flows.[386] While the third party can set financial incentives in order to 'activate' the user respectively, they potentially encounter 'double pricing' with respect to the compensation to be paid to the data holder according to Art. 9(1).[387] To achieve user empowerment more reliably, the legislator acknowledges in rec. 27 that "sector-specific needs and objectives" must be addressed by regulation, building on initiatives such as the Code of Conduct for agricultural data sharing by contractual agreement.[388]

In addition, it is questioned whether the exclusion of gatekeepers as eligible third parties in Art. 5(3) is serving innovation and the common wealth.[389] Specifically, the agglomeration of readily available data driven by market power is a concern that can manifest itself outside the realm of core platform services according to Art. 2(2) Digital Markets Act.[390] The design of Art. 5 may even give rise to (non-gatekeeper) specialised third parties aggregating data sets from the user base of a connected product.[391]

385 Cf. Bomhard, D. / Merkle, M. *RDi* 2022, 168 (171) („*nutzerakzessorischer Datenzugang*").

386 Kerber, W., *GRUR-Int.* 2023, 120 (125).

387 See below VI. 4. as well as Krämer, J., Improving The Economic Effectiveness of the B2B and B2C Data Sharing Obligations in the Proposed Data Act, CERRE, 2022, pp. 15, 21. Cf. also Specht-Riemenschneider, L., *MMR* 2022, 809 (823); Max Planck Institute for Innovation and Competition, Position Statement, 2022, pp. 27 et seq. n. 69 et seq.

388 For an in-depth analysis of the ramifications of the Data Act for precision farming and agricultural data, cf. Atik, C., 'Data Act: Legal Implications for the Digital Agriculture Sector', 2022 (SSRN pre-print).

389 Krämer, J., Improving The Economic Effectiveness of the B2B and B2C Data Sharing Obligations in the Proposed Data Act, CERRE, 2022, pp. 25 et seq.

390 For agriculture, e.g., Atik, C., 'Data Act: Legal Implications for the Digital Agriculture Sector', 2022 (SSRN pre-print), p. 16.

391 Kerber, W., *GRUR-Int.* 2023, 120 (130 n. 80).

Significant Overlaps Between the Regulatory Architectures of User and Third-Party Access

With respect to the parameters of access, Art. 5(1) largely follows the design of Art. 4(1)[392] ("without undue delay, of the same quality as is available to the data holder, easily, securely, free of charge to the user, in a comprehensive, structured, commonly used and machine-readable format and, where relevant and technically feasible, continuously and in real-time") – albeit with two notable differences. First, by referencing Art. 9 in its second sentence, Art. 5(1) highlights that (enterprise) third parties – unlike users – have to remunerate the data holder in exchange for access.[393] Second, the requirement of access "without undue delay" must be understood as applying if negotiations over the FRAND conditions of access have concluded – the possible failure of which is foreseen by Art. 5(8).[394] In this case, rec. 42 maintains that "the right to share data with third parties is enforceable in national courts or tribunals", meaning that the lack of an agreement can be overcome.[395]

The process of verifying the relevant user whose readily available data is being requested for sharing is identical between Art. 4(5) and Art. 5(4). Probably by mistake, the low threshold for a valid request ("simple request through electronic means, where technically feasible") has not been incorporated from Art. 4(1).

Eligible Third Parties / Data Recipients (Art. 2(14))

In light of the manifold similarities, Art. 5 mainly diverges from Art. 4 when it comes to the beneficiary of the right. According to rec. 33, eligible third parties encompass, *inter alia,* "an enterprise, a research organisation or a not-for-profit organisation." The third party does not have to be established in the European Union.[396] Natural persons might also qualify as third parties, provided that they are "acting for purposes which are related to [their] trade, business, craft or profession". Consumers (cf. Art. 2(23)) therefore should not fall within this definition.

392 Cf. above V. 2; other complementary provisions are found in Art. 6(2)(e) and Art. 6(2)(f).
393 Heinzke, P., / Herbers, B. / Kraus, M., *BB* 2024, 649 (655).
394 Paal, B. / Fenik, M., *ZfDR* 2023, 249 (257).
395 Antoine, L., *CR* 2024, 1 (7).
396 Antoine, L., *CR* 2024, 1 (7).

Third parties, in turn, form part of the broader notion of data recipients, which is used throughout Chapter III (Art. 8-12) of the Act. The statutory definition in Art. 2(14) reads:

> "data recipient means natural or legal person, acting for purposes which are related to that person's trade, business, craft or profession, other than the user of a connected product or related service, to whom the data holder makes data available, *including a third party following a request by the user to the data holder* or in accordance with a legal obligation under Union law or national legislation adopted in accordance with Union law" (emphasis added)

By focusing on commercial characteristics ("trade, business, craft, or profession"), it appears that the definition has primarily been devised with enterprises (cf. Art. 2(24)) in mind as third-party recipients. Nonetheless, Art. 9(4) demonstrates that not-for-profit research organisations are liable to give a (reduced) compensation to the data holder.[397]

In Particular: Gatekeepers (Art. 5(3))

Bearing one of goals of the Data Act in mind, breaking up data silos, the often criticised[398] Art. 5(3) stipulates that designated gatekeepers according to Art. 3 DMA are *not* eligible third parties. Apparently, this prohibition stands even where the data holder has been designated as a gatekeeper themselves.[399] Art. 6(2)(d) further reinforces the rule by outlawing onwards sharing by the third party to a gatekeeper.

To avoid user activation to the benefit of gatekeepers, they are not allowed to

– "solicit or commercially incentivise a user in any manner, including by providing monetary or any other compensation, to make data available

397 Cf. below VI. 4.

398 IMCO, PE736.701, pp. 27 et seq. proposed to delete Art. 5(3) entirely; *ex multis,* Krämer, J., Improving The Economic Effectiveness of the B2B and B2C Data Sharing Obligations in the Proposed Data Act, CERRE, 2022, pp. 25 et seq.; Martens, B., 'Pro- and anti-competitive provisions in the proposed European Union Data Act', 2022, pp. 14 et seq.; with a positive view on Art. 5(3): Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 34 n. 91.

399 Voicing doubts over this ambiguity: Martens, B., 'Pro- and anti-competitive provisions in the proposed European Union Data Act', 2022, p. 15.

to one of its services that the user has obtained pursuant to a request under Article 4(1)" (Art. 5(3)(a))
– "solicit or commercially incentivise a user to request the data holder to make data available to one of its services pursuant to paragraph 1 of this Article" (Art. 5(3)(b))
– "receive data from a user that the user has obtained pursuant to a request under Article 4(1)" (Art. 5(3)(c))[400]

Rec. 40 points to the legislator's motivation for excluding gatekeepers from the data access regime established by the Act:

> "Start-ups, small enterprises, enterprises that qualify as a medium-sized enterprises […] and enterprises from traditional sectors with less-developed digital capabilities struggle to obtain access to relevant data. This Regulation aims to facilitate access to data for those entities, while ensuring that the corresponding obligations are as proportionate as possible to avoid overreach. At the same time, a small number of very large enterprises have emerged with considerable economic power in the digital economy through the accumulation and aggregation of vast volumes of data and the technological infrastructure for monetising them. Those very large enterprises include undertakings that provide core platform services controlling whole platform ecosystems in the digital economy and which existing or new market operators are unable to challenge or contest."

Importantly, rec. 40 goes on to clarify that gatekeepers still have the option (within the limits of purpose / contract specificity set by Art. 4(14)) to obtain data by contractual arrangements with data holders:

> "As voluntary agreements between gatekeepers and data holders remain unaffected, the limitation on granting access to gatekeepers would not exclude them from the market or prevent them from offering their services."

In Particular: Data Intermediaries

Pursuant to Art. 5(1), a request to share data with a third party does not need to be made by the user, but can also be submitted by a party acting on the behalf of the user. Rec. 30 explain that this includes data intermediation

400 On Art. 5(3)(c) and its misplaced position in the statutory text, cf. already sub V.3.

services within the meaning of Art. 2(11) DGA (cf. Art. 2(10)). Rec. 33 elaborates on the catalysing role of data intermediaries:

> "Business-to-business data intermediaries and personal information management systems (PIMS) [pursuant to Art. 10(a) and (b) DGA] may support users or third parties in establishing commercial relations with an undetermined number of potential counterparties for any lawful purpose falling within the scope of this Regulation. They could play an instrumental role in aggregating access to data so that big data analyses or machine learning can be facilitated, provided that users remain in full control of whether to provide their data to such aggregation and the commercial terms under which their data are to be used."

Against this backdrop, it is conceivable that data intermediaries could help groups of users commercialise readily available data by aggregating and forwarding them to (other) third parties in return for payment of an appropriate fee.[401] Such a form of monetisation is more likely to succeed if the user does not merely authorise the data intermediary to make the sharing request on their behalf, but if they cede their access and sharing rights (with regard to non-personal data).[402]

Exemption for the Testing of Products not yet Placed on the Market (Art. 5(2))

Art. 5(2) stipulates that the right to third-party access does not apply where "readily available data in the context of the testing of new connected products, substances or processes that are not yet placed on the market unless their use by a third party is contractually permitted." According to Art. 2(22), the relevant "placing on the market" relates to the first time the connected product has been made available on the Union market.

The provision somewhat resembles Art. 31(2), which exempts non-production versions of data processing services from falling under the scope of the switching-related rights and obligations.

401 Richter, H., *GRUR-Int*. 2023, 458 (469) (discussing the original draft of Art. 6(2)(c)).
402 On that prospect, cf. Wiebe, A., *GRUR* 2023, 1569 (1572); cf. also Hennemann, M. / Steinrötter, B., *NJW* 2024, 1 (6).

Data Protection Law (Art. 5(7)-(8), Art. 5(13))

The interface of the right to third-party access with data protection law is covered by Art. 5(7), (8) and (13).

Art. 5(7) is drafted in parallel to Art. 4(12).[403] Consequently, the sharing of personal data is contingent upon a valid legal basis for processing in line with Art. 6 GDPR (and, if applicable, Art. 9 GDPR or Art. 5(3) of the ePrivacy Directive, cf. rec. 36).

Art. 5(8) confirms that the Act does not touch the exercise of rights of the data subject under the GDPR, especially the right to have one's personal data ported to another controller pursuant to Art. 20(2) GDPR.[404] The provision thereby expands on the juxtaposition of Art. 20 GDPR and the data access regime offered by the Act that is laid down in Art. 1(5).

Art. 5(13) (additionally) confirms that the right according to Art. 5(1) "shall not adversely affect data protection rights of others pursuant to the applicable Union and national law on the protection of personal data". Some commentators had favoured a broader exception modelled after Art. 15(4) GDPR and Art. 20(4) GDPR, namely that rights and freedoms (i.e., beyond a data protection context) should not be adversely affected.[405]

Trade Secrets (Art. 5(9)-(11))

The data holder can raise the protection of trade secrets as a defence in almost the same way as under Art. 4(6)-(8).[406] However, Art. 5(9) differs in that it limits disclosure of applicable data sets "to the extent that such disclosure is strictly necessary to fulfil the purpose agreed between the user and the third party."

This rule has been widely criticised for creating legal uncertainty.[407] It is unclear from the outset how and why the data holder should be aware of the purpose laid down in a contract that they are not part of. One might read into the norm that the user has the obligation to disclose the purpose to the data holder. In addition, Art. 5(10) rightly seems to assume that there

403 See above V.3.
404 Cf. above V.3. and rec. 35 for a legislative account reflecting on the exact scope of Art. 20 GDPR.
405 E.g. Specht-Riemenschneider, L., *MMR-Beil.* 2022, 809 (819).
406 Cf. above V.3.
407 E.g. Schweitzer, H. / Metzger, A., *ZEuP* 2023, 42 (76).

will always be – in line with Art. 8 – a contractual agreement (including a non-disclosure agreement) between data holder and data recipient and therefore a point of contact to clarify the purpose. In order not to thwart the limitation under Art. 5(9) to the detriment of data holders, the purpose in the agreement between users and third parties must be specific to a sufficient degree.[408] Because the data holder is not privy to this agreement as the "other contracting party", unfair terms control pursuant to Art. 13(5) (b) will be effective if the purpose has been disclosed to or is incorporated in the NDA with the data holder.[409]

Implicit (Second) Data License Agreement

The exercise of the right to third-party access goes along with a contractual agreement (a second data license agreement between the user and the third party regarding the use of the data according to Art. 6(1)[410])) – and which might be accompanied by an NDA pursuant to Art. 5(9).

Art. 5 does not clearly state how access (and / or the data license agreement) can be terminated. Rec. 38, however, spells out that "[i]t should be as easy for the user to refuse or discontinue access by the third party to the data as it is for the user to authorise access."

2. Obligations of Third Parties (Art. 6)

Art. 6 spells out the obligations of data recipients which receive data on the basis of Art. 5(1). These are partly linked to an agreement between the user and the data recipient (Art. 6(1) implicitly highlights the fact (or better: the necessity) of an agreement between user and data recipient); partly, the obligations are to be committed independently of an / the agreement. Many aspects of Art. 6 are related to the user's right of access under Art. 4, therefore some conflicts can be considered (and resolved) in parallel.[411]

408 Pauly, D.A. / Wichert, F. / Baumann, J., *MMR* 2024, 211 (214).
409 Further, including on the interplay with Sec. 307 German Civil Code, cf. Graf von Westphalen, F., *BB* 2024, 515 (520).
410 Heinzke, P., / Herbers, B. / Kraus, M., *BB* 2024, 649 (650).
411 Schmidt-Kessel, M., *MMR-Beil. 2024*, 75 (80 et seq.).

Non-Exclusivity

With or without an agreement, the data recipient shall not – according to Art. 6(2)(h) – "prevent the user that is a consumer (…) from making the data it receives available to other parties". Doubts from an Economics perspective have been brought forward whether and to what extent the non-exclusivity does set negative incentives for data brokers.[412] The wording "that is a consumer", which was added only in the trilogue, is an expression of the intended protection of consumers, who are to be guarded in their decisions to switch between services and products.[413]

Limited Use / Non-Compete / Security

According to Art. 6(1), a third party may only use the data made available (1) for the purposes and under the conditions agreed with the user and (2) subject to Union and national law on the protection of personal data including the rights of the data subject (Art. 12 et seq. GDPR) insofar as personal data are concerned.[414] The wording does not clearly state whether the purpose must be agreed between the user and the data holder or between the user and the third party. However, it must be based on the agreement between the user and the third party, as otherwise it would be a contract to the disadvantage of third parties.[415]

Under Art. 6(2)(b), the data recipient may not "use the data it receives for the profiling, unless it is necessary to provide the service requested by the user".[416] Rec. 39 seems to be even stricter when referring to "processing activities [that] are strictly necessary to provide the service requested by the user, including in the context of automated decision-making".[417]

412 Krämer, J., Improving The Economic Effectiveness of the B2B and B2C Data Sharing Obligations in the Proposed Data Act, CERRE, 2022, p. 21.
413 Cf. rec. 38 and 40.
414 Rec. 37 is even narrower: "In order to prevent the exploitation of users, third parties to whom data has been made available at the request of the user should process those data only for the purposes agreed with the user and share them with another third party only with the agreement of the user to such data sharing."
415 Schmidt-Kessel, M., *MMR-Beil. 2024*, 75 (80).
416 The wording "(...) for the profiling of natural persons (...) [Art. 4(4) GDPR] (...)" provided for during the procedure did not come to be adopted in the final version.
417 Cf. also Council Presidency 2022/0047(COD) – 15035/22, p. 46 in this regard.

According to the highly debated[418] Art. 6(2)(e), the data recipient may not use the received data to develop a competing product or share the data with another third party for that purpose. In addition, third parties shall not use any product data to derive insights about the economic situation, assets and production methods of, or use by, the data holder. However, the third party is allowed to develop a non-competing new and innovative product or related service (rec. 39). This is one of the aforementioned aims of the Act, namely to drive innovation in the aftermarket.

Third parties are not permitted to use the data in a manner that has an adverse impact on the security of the connected product or related service (Art. 6(2)(f)). The provision, which was added in the final version, is not explained in detail in the recitals. What exactly "the security" of the product or service constitutes remains unclear, but is likely targeted at the security of the product or service itself.

In addition, Art. 6(2)(g) stipulates that a data recipient shall not disregard the specific measures agreed with a data holder or with the trade secrets holder pursuant to Art. 5(9).

Passing-On of Data

Art. 6 also regulates the passing-on of received data by third parties. This is not permitted in principle. However, it is possible if it has been contractually agreed with the user (Art. 6(2)(c)). This indicates that the user and the third party might also agree on a general passing-on to a third party, e.g., for a 'sale' of the data.[419] In addition, the third party must take all measures to protect trade secrets.

As outlined above, Art. 5(3) excludes the transfer of data to gatekeepers as third parties. As a consistent continuation, Art. 6(2)(d) prohibits the transfer of data by third parties to gatekeepers.

418 Cf. Krämer, J., Improving The Economic Effectiveness of the B2B and B2C Data Sharing Obligations in the Proposed Data Act, CERRE, 2022, pp. 13 et seq., 23 et seq.; Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 35 n. 94.

419 Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 7 n. 14. Cf. also Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 98.

Erasing Data

Above the aforementioned limitations is the general requirement for third parties to erase[420] the data received if it no longer fulfils the agreed purpose. This can also be waived by agreement with the user.[421] Rec. 39 clarifies that this duty "complements the right to erasure of the data subject pursuant to [Art. 17 GDPR]".

Impairing Decision-making

Art. 6(2)(a) provides for particularly far-reaching protection of the user's autonomy. According to this provision, the exercise of the user's choices or rights under Art. 5 and 6 must not be made excessively difficult. In this regard, users must not be offered choices in a non-neutral manner or be deceived, coerced or manipulated. When exactly this is the case will have to be determined by jurisdiction in each individual case. The Data Act uses the term 'dark patterns' in this context, which are defined as design techniques that pressure or deceive consumers into making decisions that have negative consequences for them (rec. 38). However, common and legitimate business practices should not be regarded as dark patterns. The distinction will also have to be made on a case-by-case basis.

3. Conditions between Data Holder and Data Recipient

Complementing the access rights and the aforementioned material restrictions, Chapter III sets out requirements concerning the contractual content of data sharing agreements. The provisions of the chapter only apply in business-to-business constellations (Art. 12(1)). The data sharing must be based on FRAND principles (Art. 8) and compensations should be agreed fairly and transparently (Art. 9). Chapter III also sets out a (more or less concrete) system for alternative dispute resolution (Art. 10) and deals with secure data transmission through technical standards (Art. 11).

420 Until shortly before finalisation, the provision spoke of "to *delete*".
421 This again demonstrates the strong user-centricity of the Data Act.

FRAND-System

In case of a data access in business-to-business-relations under Art. 5 or under other Union law or national legislation adopted in accordance with Union law, Art. 8(1) sets out the principle of a **f**air, **r**easonable **a**nd **n**on-**d**iscriminatory access (FRAND). The Data Act hereby is seeking to establish a system of fair data sharing.[422] Rec. 42 describes the FRAND-system as "general access rules", which do not apply to obligations regarding data access under the GDPR. Since the FRAND rules represent a link between mandatory access rights and the contractual arrangement, they are an obligation of the data holder.[423] FRAND terms are an already known element in competition law and IP law – and can also be found in Art. 6(11) Digital Markets Act.[424] Despite the restrictive rules, the Data Act recognises the parties' freedom of contract (rec. 43).

Scope of Application

Art. 8 applies to data sharing obligations under Art. 5 or under other applicable Union law or national legislation adopted in accordance with Union law. Further, the indeterminacy of the scope of Chapter III has been criticised, since the "provision of data to a data recipient" can fall under different legal acts of the EU, in particular the DMA.[425] It was therefore proposed to clarify that Chapter III applies to obligations to make data available *only* where a reference to the Data Act is to be found.[426] This does not, however, fulfil the purpose of the Data Act as a horizontal regulation. The opening of the FRAND system is particularly relevant for further sector-specific data provision obligations following the Data Act.[427]

In temporal regard, Art. 50(4) clarifies that Chapter III (and hence also Art. 8) only applies to provision obligations that arise after the date of ap-

422 Cf. rec. 5 and 42.
423 Wiebe, A., *GRUR* 2023, 1569 (1572 et seq.).
424 Cf. Ducuing, C. / Margoni, T. / Schirru, L. (ed.), *CiTiP Working Paper* 2022, 32.
425 Ducuing, C. / Margoni, T. / Schirru, L. (ed.), *CiTiP Working Paper* 2022, 44 et seq.
426 Ducuing, C. / Margoni, T. / Schirru, L. (ed.), *CiTiP Working Paper* 2022, 45; cf. also for further proposals Schweitzer, H. / Metzger, A. / Blind, K. / Richter, H. / Niebel, C. / Gutmann, F., The legal framework for access to data in Germany and in the EU, BMWK, 2022, pp. 224 et seq.
427 Louven, S., *MMR-Beil.* 2024, 82 (83).

plication of the Data Act the 12 September 2025. Data provision obligations that arise before this date are therefore not covered.

Relationship to Art. 13

It is not entirely clear whether the provisions of Art. 8 et seq. alone or also Art. 13 apply in case of data transfer to recipients. Partially, it was considered that Art. 8 et seq. had priority.[428] However, the parallel applicability of both provisions results from the wording of Art. 8(1) and (2).[429] According to the latter provision, a contractual term of an agreement "shall not be binding if it constitutes an unfair contractual term within the meaning of Article 13 (…)".[430]

FRAND Conditions

Art. 8(1) does not establish a contractual obligation to provide data, but presumes it.[431] The rather vague general FRAND conditions from Art. 8(1) initially offer the advantage of flexibility. Yet, it is argued that FRAND terms might not be a sensible solution in many cases covered by the Act.[432] It might prove to be difficult for law enforcers and courts to create general principles in order assess FRAND terms[433], starting by stating a definition for the term 'fair', which is not provided by the proposal.[434] Since FRAND conditions are familiar from European competition and intellectual property law, the principles developed there (by the ECJ) could be transferable to the Data Act. In particular, formal negotiation obligations and obligations to co-operate must be observed, the compliance of which must be examined on a case-by-case basis.[435] FRAND therefore relates more to pro-

428 In this sense Metzger, A. / Schweitzer, H., *ZEuP* 2023, 42 (67).
429 Schwamberger, S., *MMR-Beil.* 2024, 96 (97); cf. also Wiebe, A., *GRUR* 2023, 1569 (1573).
430 See more on this under VII.
431 Louven, S., *MMR-Beil.* 2024, 82 (83).
432 Ducuing, C. / Margoni, T. / Schirru, L. (ed.), *CiTiP Working Paper* 2022, 35.
433 Max Planck Institute for Innovation and Competition, Position Statement, 2022, pp. 36 et seq. n. 99; Metzger, A. / Schweitzer, H., *ZEuP* 2023, 42 (67 et seq.).
434 Vbw, Data Act – Anpassungsbedarf aus Sicht der Bayerischen Wirtschaft, 2022, p. 13.
435 Cf. in detail Louven, S., *MMR-Beil.* 2024, 82 (84).

cedural positions than to material content.[436] *One* basic principle will not be able to cover all constellations. As a result, it will come down to a relative FRAND definition[437], which will also have to be filled in by jurisdiction on a case-specific basis.

Terms to the Detriment of the User

Art. 8(2) stipulates, in addition to the reference to Art. 13, that a contractual term of an agreement "shall not be binding if (…) to the detriment of the user, it excludes the application of, derogates from or varies the effect of the user's rights under Chapter II". The wording of the provision is almost identical to Art. 7(2). Although the provision does not explicitly stipulate it, it only refers to the provision of data in accordance with Art. 5 or a provision of data in accordance with another Union provision, but not to the provision of data on a voluntary basis.[438] This follows from its systematic position under Art. 8(1), which only refers to these forms of data provision.

Prohibition of Discrimination

Art. 8(3), which is modelled on Art. 102 TFEU[439], states that a data holder is not allowed to discriminate "between comparable categories of data recipients, including partner enterprises or linked enterprises…" (this formulation raises ambiguities[440]). When a data recipient asserts a term to be discriminatory, the data holder shall without undue delay[441] provide the data recipient, upon its reasoned request, with information showing

436 Wiebe, A., *GRUR* 2023, 1569 (1572 et seq.).
437 Louven, S., *MMR-Beil.* 2024, 82 (84).
438 Specht-Riemenschneider, L., *MMR-Beil.* 2022, 809 (820).
439 Picht, P.G., Caught in the Acts – Framing Mandatory Data Access Transactions under the Data Act, further EU Digital Regulation Acts, and Competition Law, 2022, 21.
440 Weizenbaum Institute for the Networked Society, Position paper regarding Data Act, 2022, p. 15.
441 The temporal component was included during the procedure, cf. Council Presidency 2022/0047(COD) – 13342/22, p. 45; ITRE PE732.704, p. 41. It remains questionable whether the passage achieves the intended purpose, because it does not contain any further information on what specific information must be shared.

that there has been no discrimination (Art. 8(3)). This burden of proof rule results from the consideration that the data recipient generally has no insight into the structures of the data holder and therefore does not know whether conditions are discriminatory.[442] In contrast to Art. 9(7), this also means that the data recipient must proactively point out the possibility of discrimination.[443] The use of different conditions for different data recipients may be justified if there are objective reasons (rec. 45).

It was objected that the formulation of the FRAND concept as a unilateral obligation (of the data holder) could gain the risk of a superior standing of the data recipient.[444] Therefore, in the legislative process it was proposed to reformulate the rule as mutual obligation of both parties, so private law courts and the dispute settlement bodies of Art. 10 could enforce the FRAND concept also against the data recipient where it is needed.[445] However, the proposal was finally not considered.

Provision Only at the User's Request

According to Art. 8(4)[446], a data holder shall not make data available to a data recipient, including on an exclusive basis, unless otherwise requested by the user under Chapter II. The word "including" was not initially intended and was only added in the final version. As a result, the purpose of the provision is not entirely clear.[447] While Art. 8(1) used to be a pure prohibition of exclusive access to data (which should strengthen the broad provision of data intended by the Data Act)[448], it now provides for a general ban unless permission is granted. This means that any provision of data without a user request is unlawful.

442 Cf. rec. 45.
443 Louven, S., *MMR-Beil.* 2024, 82 (84).
444 Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 39 n. 103.
445 Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 39 n. 103.
446 ITRE PE738.548, p. 67 sought to delete the entire paragraph.
447 Cf. in detail Louven, S., *MMR-Beil.* 2024, 82 (84 et seq.).
448 Hennemann, M. / Steinrötter, B., *NJW* 2022, 1481 (1484); Specht-Riemenschneider, L., *MMR-Beil.* 2022, 809 (822).

More Information than Necessary

According to Art. 8(5), data holders and data recipients shall not be required to provide more information than necessary in order to be compliant with the terms agreed or their obligations under the Data Act or other applicable Union law or national legislation adopted in accordance with Union law. The exact information that may be requested is not specified and depends on the individual case. Furthermore, it remains unclear whether the provision only addresses the contractual parties or also law enforcement or courts.[449]

Respect of Trade Secrets

The highly debated Art. 8(6) states that unless otherwise provided by Union law, including Art. 4(6) and 5(9)[450] or by national legislation adopted in accordance with Union law, an obligation to make data available to a data recipient shall not oblige the disclosure of trade secrets (within the meaning of Directive (EU) 2016/943).[451]

In the legislative process it has been critically emphasised that Art. 8(6) handles trade secrets, which should be left to the legal systems of the member states.[452] Therefore, it was argued to delete Art. 8(6) completely (which, however, was not successful).[453]

In principle, it must be examined carefully whether data contain a trade secret.[454] However, it has been criticised that Art. 8(6) could "invite" data holders not to share data arguing that otherwise trade secrets would be

449 Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 39 n. 105.

450 The Council Presidency and the Committee on Industry, Technology and Energy (ITRE) have proposed the harmonisation of Art. 4(3) and Art. 5(8) with Art. 8(6) in order to clarify that there is no obligation to share trade secrets with a data recipient except in the cases expressly provided by law, cf. Council Presidency 2022/0047(COD) – 13342/22, p. 45; ITRE PE732.704, p. 41.

451 Directive (EU) 2016/943 of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure.

452 Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 102 n. 284.

453 Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 39 n. 106.

454 For the German GeschGehG cf. Heinzke, P., *BB* 2023, 201 (205 et seq.).

revealed.[455] In that case, the Art. 5 et seq. are in danger to miss their objectives as data holders could try to blur data extensively. As a minimum, it can be expected that the general conditions for the existence of a trade secret must be stated or explained.

Specht-Riemenschneider has criticised the general priority of trade secrets in Art. 8(6) and Art. 5(9). The protection of trade secrets could also be ensured by blacking out or pseudonymising sensitive data, without completely refraining the sharing of non-personal data.

4. Compensation

The data economy is rarely characterised by altruistic motives, but (like other markets) by profit interests. The Data Act pushes data flows between data holder and data recipient under strict conditions by the Art. 5 and 6. The closely related question of whether data holders can demand compensation for this obligation is answered in Art. 9. The provision presupposes the possibility of agreeing compensation and makes specifications for their structure.[456] The Data Act does not stipulate that this must be a monetary compensation.[457] Other forms of remuneration are therefore also possible.

To avoid compensation, the Data Act does not hinder the user to request the data free of charge according to Art. 4(1) by himself – and then forward the data on to third parties.[458] This 'easy way out' has been widely criticised.[459] The way is, however, only 'easy' if the user takes the technical burden – and has the technical capabilities – to access, store, and forward the respective data. Especially in the consumer segment, this will regularly not be the case.

455 Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 39 n. 106; Krämer, J., Improving The Economic Effectiveness of the B2B and B2C Data Sharing Obligations in the Proposed Data Act, CERRE, 2022, p. 21.

456 Cf. also rec. 46.

457 Louven, S., *MMR-Beil.* 2024, 82 (85).

458 Bomhard, D. / Merkle, M., *RDi* 2022, 168 (171).

459 Krämer, J., Improving The Economic Effectiveness of the B2B and B2C Data Sharing Obligations in the Proposed Data Act, CERRE, 2022, pp. 16 et seq.; Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 29 n. 72.

General Provisions

Art. 9(1) states that any "compensation agreed upon between a data holder and a data recipient for making data available in business-to-business relations shall be non-discriminatory and reasonable and may include a margin".

The key terms are not further defined. Initially, it is not clear what exactly 'reasonable' means. The provision does not state calculation methods or examples. This was the subject of lively debates during the legislative process.[460] From a practical and an Economics perspective it has been argued that it will be difficult to determine a respective compensation – and that corresponding lengthy negotiations and / or court proceedings are highly likely.[461] To counterbalance respective challenges, a rebuttable presumption of a zero-access price was proposed in the literature.[462]

Notably, Art. 9 does not define an upper or lower limit for compensation, meaning that it is possible for compensation to be as high as possible, but also close to zero.[463] Although Art. 9(2) contains general criteria that must be taken into account with regard to compensation (see below), it will primarily be the dispute settlement bodies under Art. 10 and courts that will be concerned with respective questions and will draw up guidelines.[464] To determine reasonableness, comparable market prices or market-orientated approaches from market practice could, however, serve as a basis.[465] In this context, it is important to emphasise the prohibition of overcompensation. This results from the (admittedly vaguely formulated) parameters of Art. 9. The compensation can be demanded therefore *only* for the provision.[466]

460 Cf. ITRE PE739.548, pp. 69 et seq.; LIBE PE737.389, p. 46; ITRE PE738.548, pp. 69 et seq.; ITRE PE738.548, p. 70; ITRE PE738.548, p. 72.

461 Krämer, J., Improving The Economic Effectiveness of the B2B and B2C Data Sharing Obligations in the Proposed Data Act, CERRE, 2022, pp. 15 et seq.

462 See Krämer, J., Improving The Economic Effectiveness of the B2B and B2C Data Sharing Obligations in the Proposed Data Act, CERRE, 2022, p. 24. Cf. also Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 29 n. 72.

463 Louven, S., *MMR-Beil.* 2024, 82 (85).

464 Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 37 n. 101.

465 Cf. in detail Louven, S., *MMR-Beil.* 2024, 82 (85 et seq.).

466 Cf. in detail Louven, S., *MMR-Beil.* 2024, 82 (86).

Furthermore, it is unclear what 'non-discriminatory' means in the context of Art. 9. It is worth considering whether the criteria from Art. 8 can be transferred.[467]

Finally, the Act makes a crucial distinction between the costs of providing data and a margin. The data holder may therefore make a profit from the provision of data.[468] Such profit is first of all limited by the criteria 'reasonable' and, second, can be limited or completely excluded by Union regulations, Art. 9(6).[469]

Compensation Factors

Art. 9(2) specifies concrete details on how the compensation can be determined. Firstly, the "costs incurred in making the data available, including, in particular, the costs necessary for the formatting of data, dissemination via electronic means and storage" should be considered (Art. 9(2)(a)).[470] Furthermore, investments in the collection and production of data should be taken into account and the fact whether other parties contributed to obtaining, generating or collecting the data in question (Art. 9(2)(b)). A compensation can also depend on the volume, format and nature of the data (Art. 9(3)). According to the wording, the enumeration is neither obligatory nor exhaustive. It is therefore imaginable that other costs and circumstances on the part of the data holder may also have an impact on the compensation.[471]

Micro, Small, And Medium-Sized Enterprises

The Data Act recognises an increased need for the protection of SME.[472] Therefore, Art. 9(4) states that they shall not be charged a margin or other compensation in excess of the directly related costs of providing the data as described in Art. 9(2)(a). This also applies to non-profit organisations.

467 In favour of this Louven, S., *MMR-Beil.* 2024, 82 (85).
468 Louven, S., *MMR-Beil.* 2024, 82 (85).
469 See below for the requirements.
470 This wording is partly based on the amendment proposed by the Council Presidency, cf. Council Presidency 2022/0047(COD) – 13342/22, p. 45.
471 Cf. Louven, S., *MMR-Beil.* 2024, 82 (85).
472 Cf. rec. 49.

Specht-Riemenschneider concludes from this that the compensations should not be understood as payment for the concrete data, but as an actual "equalisation" for the costs incurred and investment required for making the data available.[473]

The limitation set by Art. 9(4) can put large companies at a massive disadvantage and is consequently criticised on this ground.[474] On the other hand, it was argued that the cost-based approach was more in line with the objectives of the Data Act and that the limitation should be applied to all types of data recipients.[475]

Art. 9 does not provide for any special rules for cases in which SMEs themselves are data holders. This has been criticised because, if SMEs share data with each other, no profit can be made and the growth of the company may suffer as a result.[476]

Due to the increased relevance of data intermediaries in the supply of data, it was partially proposed (but not adopted) to put data intermediaries with regard to compensations on the same level as SME.[477] This would have been in line with the DGA's aim to promote data intermediaries (cf. rec. 27 DGA).

Guidelines on the Costs

The Commission shall adopt guidelines on the calculation of reasonable compensation (Art. 9(5)). In doing so, it shall recognise the advice of the EDIB (cf. Art. 42).

It is not fully clear to which compensations these guidelines relate. The open wording suggests that the guidelines refer to all compensation within the meaning of Art. 9, whereas the systematic position of the paragraph suggests that they refer only to Art. 9(4), i.e. to the compensation of SMEs and non-profit research organisations.

473 Specht-Riemenschneider, L., *MMR-Beil.* 2022, 809 (822).
474 BDI Stellungnahme zum Legislativvorschlag des EU-Data Act, 2022, p. 16.
475 ITRE PE739.548, p. 74 therefore wanted to change the wording to „Any reasonable compensation(…)".
476 Vbw, Data Act, Anpassungsbedarf aus Sicht der Bayerischen Wirtschaft, 2022, p. 18; Bitkom, 'Bitkom Position Paper EU Data Act Proposal' (19 April 2022), 2022, p. 6.
477 MyData Global response of the Data Act, 2022, p. 5.

Exclusion of Compensation

Art. 9(6) allows Union law or national legislation adopted in accordance with Union law to exclude compensation for making data available or providing for lower compensation. For these cases, rec. 50 sets up higher requirements for compensations, namely the need to ensure consumer participation and competition or to promote innovation in certain markets.[478] Thus, rec. 50 underlines that compensation should generally be negotiated by the parties themselves. Their regulation shall be the exception.

Information

To ensure the compliance of compensation terms with the paras. 1 to 4, Art. 9(7) stipulates an obligation for the data holder to provide the data recipient with information containing the calculation of the compensation in a sufficiently detailed form.[479] Rec. 51 underlines the principle of transparency respectively.

Calculation

In the Commission's proposal, neither the text of the regulation nor the recitals provided concrete calculation criteria, which was heavily criticised.[480] Although there are quite concrete factors for the calculation, it might remain difficult to 'find' a respective compensation in dispute settlement scenarios or before courts.[481] A major hurdle in the calculation of the consideration is especially the "convertibility" of the data. The costs of

478 The ITRE Draft Report proposed to delete Art. 9(6) in its entirety to ensure a coherent structure of the Data Act as a horizontal framework; cf. ITRE PE732.704, pp. 42 et seq.

479 While the Commission's draft spoke of the data recipient's possibility "to verify that the requirements of para. 1 and, where applicable, para. 2 are met" the Council Presidency proposed to use a more neutral wording that states the data recipient's possibility to "assess whether the requirements of…" cf. Council Presidency 2022/0047(COD) – 15035/22, p. 49.

480 Cf. e.g. Gerpott, T., *CR* 2022, 271 (279) or Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 104.

481 Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 104.

collecting and transmitting the data are typically relatively low, while the collected data later have a high commercial value.[482] In this regard, it is considered whether a complete waiver or a flat-rate reimbursement in the amount of a few Euros would be more expedient than concrete calculation in individual cases, particularly in order to avoid the disruptive potential of concrete cost calculation.[483]

5. Dispute Settlement

In case of disagreements regarding the sharing of data in accordance with Art. 4 et seq. or the FRAND conditions in Art. 8 or with regard to compensations, the parties under the Data Act are at free rein to consult (state) courts for dispute resolution.[484] However, these classic contradictory processes could be connected with practical difficulties in enforcement and intensive (and costly) measures, which are not always intended. The Data Act therefore introduces the idea of independent dispute settlement bodies to which the Act's actors can turn. This alternative (and therefore simpler) way to resolve disputes should benefit data holders and data recipients and thereby strengthen trust in data sharing (rec. 52). The dispute settlement bodies should offer simple, fast and low-cost ways to do this. There is neither an obligation of the member states to establish dispute settlement bodies (rec. 52) nor an obligation of the authorised parties to use them (rec. 53). This dispute settlement system is regulated in Art. 10 and will be discussed in the following.[485]

From the start of the legislative process, Art. 10 has contained a number of gaps and ambiguities, particularly with regard to the practical implementation of the procedures.[486] Even though details have changed in the course of the legislative process (particularly with regard to the personal scope of application), many of the identified weaknesses remained, such as inadequate rules on international jurisdiction, a lack of procedural rules or harmonisation requirements.

482 Podszun, R., Der EU Data Act und der Zugang zu Sekundärmärkten am Beispiel des Handwerks, 2022, p. 52.
483 Podszun, R., Der EU Data Act und der Zugang zu Sekundärmärkten am Beispiel des Handwerks, 2022, pp. 54 et seq.
484 Cf. Art. 4(3), 4(9) or 5(12).
485 For a deep insight cf. Weiß, R., *MMR-Beil.* 2024, 101.
486 Cf. especially Niedermaier, T. / Picht, P., FRAND ADR under the Data Act and the SEP Regulation, 2022.

Personal Scope

Art. 10(1) states that "[u]sers, data holders and data recipients shall have access to a dispute settlement body (...) to settle disputes pursuant to [Art.] 4(3) and (9) and [Art.] 5(12) as well as disputes relating to the fair, reasonable and non-discriminatory terms and conditions for, and transparent manner of, making data available in accordance with this Chapter and Chapter IV".[487]

An access to dispute resolution bodies for the user was added in the final version. However, the idea that the interests of the user require an equal level of protection is not new. At an earlier stage of the legislation, it was proposed that the data recipient (who were already authorised in the Commission version) should act as the user's legal representative.[488] Art. 4(3) and (9) were added as a consequence of the inclusion of the user. Art. 4(3) emphasises unrestricted access to courts in case of a dispute with the data holder about an agreement under Art. 4(2). In addition, the user may bring the complaint to the competent authority in accordance with Art. 37 (Art. 4(3)(a)). Furthermore, there is the aforementioned possibility of dispute resolution in accordance with Art. 10(1). The user has the same rights if the data holder refuses access in accordance with Art. 4(7) and (8) (Art. 4(9)).

Art. 5(12) extends these possibilities to third parties if these seek to challenge a data holder's decision to refuse or to withhold or suspend data sharing pursuant to Art. 5(10) and (11).

Art. 10(4) further expands the group of persons entitled to settlement access to customers and providers of data processing services to settle disputes relating to breaches of the rights of customers and the obligations of providers of data processing services, in accordance with Art. 23 to 31.

487 In the Commission proposal, Art. 10 was limited to Art. 8 (FRAND-terms), which was criticised, cf. Gerpott, T., *CR* 2022, 271 (279); Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 40 n. 108; Cf. ITRE PE739.548, p. 79 with the propose to take in Art. 13 in the wording. Later on, Chapter IV (Art. 13) was also included, cf. Council Presidency 2022/0047(COD) – 15035/22, p. 49.

488 IMCO PE736.701, p. 29.

Material Scope

In substance, the dispute settlement body can decide on the existence of a claim for data provision, its conditions and compensation.[489] The 'if' and 'how' of data provision are therefore reviewable.[490] The settlement bodies can decide on FRAND terms and conditions as well as on the other provisions of Chapter II (compensation and technical protection measures). Moreover, the bodies serve to determine whether contractual terms are unfair within the meaning of Art. 13.

Fees

Knowing how high the costs of proceedings under Art. 10 are plays a major role in the question of whether to pursue alternative dispute resolution. Art. 10 therefore also addresses the fees for dispute settlement. According to Art. 10(2) dispute settlement bodies shall make the fees, or the mechanisms used to determine the fees, known to the parties concerned *before* those parties request a decision. This can be particularly important for counselling practice to be able to predict the risks and benefits of alternative dispute resolution.

The question of who has to bear which costs is of particular importance. This is regulated in Art. 10(3). If the dispute settlement body decides in favour of the user or of the data recipient, the data holder has to bear all the fees charged by the dispute settlement body. Further, he has to reimburse that user or that data recipient for any other reasonable expenses that it has incurred in relation to the dispute settlement. On the other hand, if the dispute settlement body decides in favour of the data holder, the user or the data recipient has *not* to reimburse any fees or other expenses that the data holder paid or is to pay in relation to the dispute settlement, unless the dispute settlement body finds that the user or the data recipient manifestly acted in bad faith. This rule underlines the guiding principle of the Data Act according to which users and data recipients are structurally weaker and therefore worth protecting (unless they are acting "in bad faith"). However, alternative dispute resolution is intentionally not made attractive

489 In the Commission's version, the dispute settlement body's review was limited to the "how" of provision.

490 Weiß, R., *MMR-Beil.* 2024, 101.

for the data holder. This raises the question of how often settlement bodies are actually called upon in practice.[491]

Certification

Dispute settlement bodies must be certified by the member state in which they are located (Art. 10(5)). The bodies are private, state-established bodies are not intended (in contrast to the Commission draft).[492] To be certified, the body must fulfil a number of requirements. The body has to demonstrate that it is impartial and independent, and it will issue its decisions in accordance with clear, non-discriminatory and fair rules of procedure (Art. 10(5)(a)). It further must have the necessary expertise, in particular in relation to fair, reasonable and non-discriminatory terms and conditions, including compensation, and on making data available in a transparent manner (Art. 10(5)(b)). It is, however, criticised that too little expertise actually exists in this regard.[493] In addition, there is no or hardly any case law on this topic in the EU. Art. 10 also does not contain any requirements regarding the professional qualification of such settlement bodies.[494] Finally, from a technical and formal point of view, the settlement body has to enable easy access through electronic communication technology (Art. 10(5)(c)) and issue its decisions in a swift, efficient and cost-effective manner and in at least one official language of the Union (Art. 10(5)(d)).

Apart from these conditions, the Data Act does not specify further requirements. However, the member states are free to adopt more detailed provisions themselves, which also regulate questions relating to the expiry and re-certification (rec. 52).

The certified dispute settlement bodies shall be notified to the Commission (Art. 10(6)). The certified and notified dispute settlement bodies should be listed on a dedicated and updated website by the Commission.

The Commission's proposal stipulated that – in case there is no certified dispute settlement body in a member state by the 12 September 2025 – the respective state should establish and certify a settlement body which fulfils the aforementioned conditions. This provision was deleted.

491 Weiß, R., *MMR-Beil.* 2024, 101 (104).
492 Weiß, R., *MMR-Beil.* 2024, 101 (102).
493 Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 42 n. 113.
494 Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 42 n. 113.

Refusing Disputes / International Jurisdiction

According to Art. 10(7) dispute settlement bodies shall refuse a request to resolve a dispute, when the concerning dispute has already been brought before another dispute settlement body or before a court or a tribunal of a member state. The term "of a member state" will not only refer to the body that has been called upon, but to all other bodies in all member states.[495]

It has been criticised that the Art. 10 does not regulate its international jurisdiction (and rec. 52 does not either elaborate on this matter).[496] However, rec. 53 was added in the course of the legislation, which, in addition to the voluntary nature of the procedure, also clarifies that the parties may submit disputes to any dispute resolution body, whether in their own member state or in another. This right to choose freely among the settlement bodies in the EU could lead to conflicts, not at least because a party might prefer to start the conflict in the country of its domicile.[497] This again brings up the unanswered question of the application of Art. 4(1) Regulation (EU) 1215/2012 (Brussels I-bis Regulation)[498], which states the obligation to sue another party in the courts of the state of the defendant's domicile.[499] However, even when Brussels I-bis Regulation is applicable, there is a high chance that not all member states have certified settlement bodies, which raises the question, to which settlement body a dispute should be brought.[500] Due to these uncertainties, it might eventually be the wiser option to bring the dispute to a member state Court directly.[501]

495 Weiß, R., *MMR-Beil.* 2024, 101 (102).
496 Max Planck Institute for Innovation and Competition, Position Statement, 2022, pp. 40 et seq. n. 111.
497 Max Planck Institute for Innovation and Competition, Position Statement, 2022, pp. 40 et seq. n. 111.
498 Regulation (EU) 1215/2012 of the European Parliament and of the Council on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters.
499 Max Planck Institute for Innovation and Competition, Position Statement, 2022, pp. 40 et seq. n. 111.
500 Max Planck Institute for Innovation and Competition, Position Statement, 2022, pp. 40 et seq. n. 112.
501 Max Planck Institute for Innovation and Competition, Position Statement, 2022, pp. 40 et seq. n. 112.

Competences of the Settlement Bodies

Art. 10 does not define the concrete competences of the settlement bodies. This leads to significant uncertainty. In many cases, the bodies must be able to clarify both facts and legal issues, for example whether technical protection measures within the meaning of Art. 11 have been implemented or circumvented (fact) and at the same time whether these unlawfully discriminate against the data recipient (legal question).[502] As no clear limits were set in the final version either, it can be assumed that the dispute settlement bodies have a broad decision-making competence within the scope of Art. 10(1). This ranges from simple recommendations to the parties to concrete measures, such as deciding on the (non-)binding nature of a contractual term.

Rules of Procedure

Art. 10(8) states that the parties must be granted a reasonable period of time to demonstrate their point of view on matters the parties have brought before the settlement bodies and ensures the right to a fair trial under Art. 6(1) ECHR.[503] The undefined legal term of a "reasonable period of time" will have to be clarified. The parties shall also be provided with the submissions of the other party and any statement made by experts. In that context, the parties shall also be granted the possibility to comment on those submissions and statements.

A dispute settlement body shall adopt its decision within 90 days after the request pursuant to Art. 10(1) and (4). The decision has to be in writing or on a durable medium and shall be supported by a statement of reasons (Art. 10(9)).

Art. 10 does not contain any further specifications regarding the form or the procedure. Even if it is not expressly laid down, it seems possible and useful for the member states or the dispute settlement body itself to create its own rules or internal statutes that specify the procedure.

502 Niedermaier, T. / Picht, P., FRAND ADR under the Data Act and the SEP Regulation, 2022, pp. 4 et seq.

503 Weiß, R., *MMR-Beil.* 2024, 101 (103).

Annual Activity Reports

In order to create uniform 'case law' and comparability, Art. 10(10) provides that the dispute settlement bodies shall draw and make publicly annual activity reports. Those reports shall include, in particular, an aggregation of the outcomes of disputes, the average time taken to resolve and the most common reasons for disputes. To avoid unnecessary exchange of information and disputes, Art. 10(11) states that the annual reports may include recommendations as to how the respective problems can be avoided or resolved. The provision therefore does not include any coordination of the dispute resolution bodies, which would, however, be desirable in order to create a level playing field, standardised decisions and thus greater legal certainty.[504]

Decision Effects / Enforcement / Interplay with Judicial Clarification

According to Art. 10(12), the decision of the dispute settlement body only binds the parties if they have explicitly consented to its binding nature before the start of the dispute settlements proceedings. It is likely that many disputes are not brought before a dispute resolution body in the first place.[505]

Rec. 56 stipulates that the parties shall not be prevented to exercise their fundamental rights to an effective remedy and to a fair trial. In this respect, Art. 10(13) states that Art. 10 does not affect the right of the parties to seek an effective remedy before a court or tribunal of a member state. The wording "remedy" in Art 10(13) could be understood to suggest that dispute settlement has priority over state court proceedings and that only the decision of the dispute settlement body is subject to review.[506] However, it would then be unclear why the Data Act emphasises so strongly at other points that the right to make use of state courts remains unaffected (Art. 4(3) and (9), 5(12), rec. 56 second sentence).

504 Weiß, R., *MMR-Beil.* 2024, 101 (102).
505 Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 42 n. 114.
506 Apparently in this sense Weiß, R., *MMR-Beil.* 2024, 101 (103).

6. Technical Protection

Technical protective measures to be used when transferring data are addressed by Art. 11.[507] The data holder is given far-reaching (technical) protection options with equally far-reaching enforcement and intervention options in case of unauthorised use by the data recipient. This gives the data holder the *de facto*-possibility to restrict the use of the data in a selective and targeted manner. This form of 'exclusivity' has already been recognised in the literature as a construct that comes close to unintended data ownership.[508] It is not clear whether the user has a legal claim against the data holder to the implementation of technical protection measures.[509]

Art. 11 is not related to or linked to Art. 3.[510] Although both provisions deal with technical requirements in the broadest sense, the provisions regulate different complexes. Art. 11 does not impose obligations on the manufacturer, but on the data holder (which can, but does not need to the same person). Also, Art. 3 DA only addresses product data and related services data, while Art. 11 gives the data holder the possibility to protect all data by technical protection measures.

Protection Measures

Art. 11(1) "allows" for technical protection measures to prevent unauthorised access to data and to ensure compliance with Art. 4, 5, 6, 8 and 9 and the agreed contractual terms for making data available. Examples of protection measures include smart contracts and encryption, including metadata. The data holder is not obliged to use protection measures. Rather, Art. 11 sets limits for the use of respective measures.[511]

According to Art. 11(1) the implementation of the technical protection measures must fulfil three requirements. First, the measures must be "appropriate". The question of when a measure is appropriate is difficult to answer in abstract terms and depends significantly on the type and extent of the data provision. A case-by-case assessment is necessary here.[512]

507 For a deep insight cf. Steege, H., *MMR-Beil.* 2024, 91.
508 Steege, H., *MMR-Beil.* 2024, 91.
509 Ducuing, C. / Margoni, T. / Schirru, L. (ed.), *CiTiP Working Paper* 2022, 38.
510 For the following, cf. Steege, H., *MMR-Beil.* 2024, 91 (92).
511 Specht-Riemenschneider, L., *MMR-Beil.* 2022, 809 (823).
512 Steege, H., *MMR-Beil.* 2024, 91 (93).

Second, the measures shall not discriminate between data recipients. Similar to Art. 9, the question arises as to whether definitions and principles (yet to be developed) from Art. 8 are transferable for the understanding of this term. Neither Art. 11(1) nor the correlating rec. 57 explain whether and when discrimination can be justified in individual cases.[513]

Third, the measures shall not hinder a user's right to obtain a copy of, retrieve, use or access data, to provide data to third parties pursuant to Art. 5 or any right of a third party under Union law or national legislation adopted in accordance with Union law. On the one hand, it is questionable at what point the user is prevented from exercising the aforementioned rights. From the open wording, it could be concluded that an obstacle already exists if the measures are only capable of preventing the rights.[514] On the other hand, it is unclear at what level a security measure is considered to be obstructive and whether the subjective knowledge and skills of the user or those of an objective average user should be used as a yardstick.[515]

Finally, the third sentence of Art. 11(1) states that users and third parties shall not alter or remove the technical protection measures unless agreed by the data holder. Any circumvention of protection measures is unlawful. Even if it is not clear from the wording of Art. 11(1), this authorisation must be given at the time of the circumvention.[516] According to the broad wording, it also seems possible that the data holder might authorise a circumvention retrospectively.[517]

Conditions and Consequences

Art. 11(2) and (3) address the consequences for data recipients and third parties in specific scenarios. The scenarios are defined in Art. 11(3). The provision conclusively lists five settings. Art. 11(3)(a) refers to the case that a third party or a data recipient has "provided false information to a data holder, deployed deceptive or coercive means or abused gaps in the technical infrastructure of the data holder designed to protect the data" to obtain data. The broadly worded provision is (partially) focused on

513 Steege, H., *MMR-Beil.* 2024, 91 (94) raising the problem.
514 In favour of this cf. Steege, H., *MMR-Beil.* 2024, 91 (94).
515 Password protection alone will not be enough to hinder the user's rights, cf. Steege, H., *MMR-Beil.* 2024, 91 (94 et seq.).
516 Steege, H., *MMR-Beil.* 2024, 91 (93).
517 Steege, H., *MMR-Beil.* 2024, 91 (94).

the *technical* circumvention of established protective measures. Rec. 57 specifies that "misleading the data holder by providing false information with the intent to use the data for unlawful purposes" falls under the provision. However, details are not specified. Hence, it remains unclear when information is "false" or when exactly gaps have been "abused". Another technical aspect is mentioned by Art. 11(3)(d). It refers to a setting in which the technical and organisational measures agreed in accordance with Art. 5(9) have not been maintained. In the form of a general clause, Art. 11(3)(e) refers to Art. 11(1) and an alternation or removal of technical protection measures without the agreement of the data holder.

In contrast, Art. 11(3)(b) and (c) refer to unauthorised use of *the data*. According to the provisions data recipients may not use "the data made available for unauthorised purposes, including the development of a competing connected product within the meaning of [Art. 6(2)(e)]" and may not "unlawfully disclose data to another party". It is not clarified what "unlawfully" means. This will depend on the contractual agreement between the data holder and the data recipient.

It is not explicitly stated who has to *prove* whether one of the settings defined in Art. 11(3) are fulfilled.[518]

The consequences of the settings defined in Art. 11(3) are stipulated in Art. 11(2). The provision specifies – also conclusively – four measures with which the data recipient or the third party must comply if requested by the data holder, the holder of the trade secret, or the user. Art. 11(5) states that the user shall have the same rights according to Art. 11(2) if a data recipient infringes Art. 6(2)(a) or (b).

Art. 11(2)(a) and (b) refer to the erasure of the data and the termination of all activities made possible by the data. All data and copies thereof must be deleted (Art. 11(2)(a)). In addition, the data recipient can be obliged "to end the production, offering or placing on the market or use of goods, derivative data or services produced on the basis of knowledge obtained through such data, or the importation, export or storage of infringing goods for those purposes, and destroy any infringing goods, where there is a serious risk that the unlawful use of those data will cause significant harm to the data holder, the trade secret holder or the user or where such a measure would not be disproportionate in light of the interests of the data holder, the trade secret holder or the user" (Art. 11(2)(b)).

518 Cf. Gerpott, T., *CR* 2022, 271 (279).

Furthermore, the data recipient or the third party might have "to inform the user of the unauthorised use or disclosure of the data and of the measures taken to put an end to the unauthorised use or disclosure of the data" (Art. 11(2)(c)). However, the provision does not specify in detail how the user must be informed and what information is included. For example, the wording does not indicate whether it must be informed about when the data was disclosed or which parties were involved. A narrow interpretation would potentially undermine the purpose of the provision. The user should in any case be aware of the general circumstances of the "data leak" and whether these have been solved. This refers in particular to the question of *which* data is affected, *when* the incident took place, *why* the data was disclosed and *where* the data flowed to.

Finally, the data recipient or the third party might have to compensate the party suffering from the misuse or disclosure of the unlawfully accessed or used data (Art. 11(2)(d)). Excessive requests from the data holder or third parties are limited by rec. 57, according to which all requests from harmed parties shall "be assessed in the light of their proportionality in relation to the interests of the data holder, the trade secret holder or the user". This exemption is not further defined or explained.

The obligations under Art. 11(2) must be fulfilled without delay. As already outlined above, the term 'undue delay' is to be determined by union law.[519]

Altering or Removing Technical Protection by the User and others

Art. 11(4) extends the personal scope of Art. 11(2). According to the provision, also the user may neither alter nor remove the technical protection measures taken by the data holder. This also applies to the measures taken to protect trade secrets. In addition, any other party that receives data from the user violating provisions of the Data Act is subject to the obligations under Art. 11(2).

Art. 11(4) clarifies that there is no 'right to hack' for the user and can furthermore be seen as a "small crack" in the principle of user-centricity in favour of the data holder.

519 See sub. V.

Enforcement

Art. 11 does not contain any information on private enforcement (the Data Act focuses more on public enforcement (cf. Art. 40)).[520] However, Art. 11(2) (also in favour of the cases regulated by Art. 11(4) and (5)) seems to establish respective claim enforceable before a court.

Disputes under Art. 11 may be brought before a dispute resolution body within the meaning of Art. 10(5). Art. 11 is not explicitly mentioned in Art. 10(1), but is covered by the "making data available in accordance with (…) Chapter [III]" of that very provision.

7. Common Standards for Smart Contracts (Art. 36)

Hailed for their "potential to facilitate automated data sharing and pooling at scale while enforcing usage restrictions"[521], so-called smart contracts had been floated by the Commission as a high-level technical tool since the outset of the Data Act initiative. The main use case manifesting in the Act's final version concerns long-term arrangements (put differently, data licensing agreements[522]) between data holders and data recipients regularly sharing data; in these settings, smart contracts are envisioned to decrease transaction costs (rec. 47).

Smart contracts are chiefly mentioned (and put into concrete terms) by Art. 36. They also appear in two other regulatory contexts: first, in Art. 11(1) as a protective measure against unauthorised disclosure when implementing the sharing of readily available data pursuant to Art. 4 et seq.; and second, as objects of interoperability requirements to enable the automatic execution of data licensing agreements within data spaces pursuant to Art. 33(1)(d).

The Notion of Smart Contracts

According to Art. 2(39), "smart contract" means a computer program used for the automated execution of an agreement or part thereof, using a

520 Cf. for the German private law Steege, H., *MMR-Beil.* 2024, 91 (95).
521 Commission, 'Inception Impact Assessment: Data Act', Ares(2021)3527151, p. 3.
522 Siglmüller, J., *MMR-Beil.* 2024, 112 (115).

sequence of electronic data records and ensuring their integrity and the accuracy of their chronological ordering. To some extent, the definition picks up on the classical conceptualisation by *Nick Szabo,* who in 1994 had defined smart contracts as computerised transaction protocols that execute the terms of a contract.[523] Where prior versions had tied the notion of smart contracts to the use of electronic ledgers and thus, the Distributed Ledger Technology (DLT), Art. 2(39) has rightfully abandoned the DLT and its popular epithet – the blockchain – as a necessary vehicle for smart contracts.[524] Instead, rec. 104 affirms the principle of technical neutrality, which does not preclude that smart contracts *can* be connected to an electronic ledger. Viewing smart contracts through the lens of computer programs exclusively can still be regarded, however, as a violation of technological neutrality.[525]

Essential Requirements for Smart Contracts (Art. 36(1))

When it comes to the technicalities of smart contracts, Art. 36(1) deems essential five characteristics: robustness, safe termination and interruption, data archiving and continuity, access control, and consistency with the data sharing agreement the smart contract executes. Rec. 104 clarifies that these requirements only apply to vendors of smart contracts, except where they develop smart contracts in-house exclusively for internal use. Judging from the juxtaposition in Art. 36(2), Art. 36(3), and Art. 36(9) of vendors and other persons whose business involves the deployment of smart contracts for others, it appears that vendors are indeed identified by the sale of such computer programs.

Looking at the above requirements, (rigorous) access control mechanisms feature twice in Art. 36(1)(a) and Art. 36(1)(d), which is probably due to poor drafting. Robustness under Art. 36(1)(a) is lauded in principle as the capacity to avoid functional errors and withstand third-party manipulation, but its suitability to address well-known vulnerabilities of smart contracts in practice is called into question (at least in the absence of

523 Cit. per Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 84 n. 234; for other definitions of the term, cf. Mik, E., *EuCML* 2024, 1 (1) (lamenting a "medley of inconsistent approaches").

524 Siglmüller, J., *MMR-Beil.* 2024, 112 (116).

525 Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 84 n. 234.

harmonised standards under Art. 36(5)).[526] The possibility to interrupt and safely terminate the execution of the self-executing protocol underlying the smart contract (Art. 36(1)(b)) is indispensable to allow for amendments to the otherwise immutable contract.[527] However, this goal clashes with the characteristic integrity and consistency of smart contracts (Art. 36(1)(e)) as well as their auditability (Art. 36(1)(c)), which could be thwarted should a "kill switch" become necessary to avoid future accidental executions of the protocol.[528] More generally, the consistency between the smart contract and the agreement it is meant to execute can be hard to verify from the rules as transcribed into source code.[529]

Declaration of Conformity (Art. 36(2) and (3))

Vendors of smart contracts or, failing that, persons whose business involves the deployment of smart contracts for others in the context of executing an agreement to make data available shall perform a conformity assessment to ascertain that the essential requirements under Art. 36(1) are met. Per rec. 105, the conformity assessment should observe the general principles of the Accreditation Regulation (EC) No. 765/2008. Upon a positive result of the assessment, the vendor or trader shall issue a so-called EU declaration of conformity, which pursuant to Art. 36(3) triggers their responsibility for compliance with Art. 36(1). Art. 36(3) does little in the way of linking this responsibility to (private) enforcement, nor does it specify the details of the declaration (conversely, see Annex V of the AI Act).

As for the enforceability of smart contracts themselves, there is broad consensus that the current member state law on contracts is reasonably well-equipped to accommodate smart contracts in much the same way as conventional agreements.[530]

526 Casolari, F. / Taddeo, M. / Turillazzi, A. / Floridi, L., 'How to Improve Smart Contracts in the European Union Data Act' 2:9 (2023) *Digital Society* 3.
527 Id. at 2.
528 Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 85 n. 235.
529 Mik, E., *EuCML* 2024, 1 (3).
530 Siglmüller, J., *MMR-Beil.* 2024, 112 (115 n. 27); cf. Casolari, F. / Taddeo, M. / Turillazzi, A. / Floridi, L., 2:9 (2023) *Digital Society* 4.

Harmonised Standards (Art. 36(4) and (5))

In accordance with Art. 36(5), the Commission shall request one or more of the three European standardisation organisations (CEN, Cenelec, and ETSI[531]) to draft harmonised standards on the matter of essential requirements for smart contracts raised by Art. 36(1). With some degree of redundancy, harmonised standards are defined in Art. 2(43) by reference to Art. 2(1)(c) Regulation (EU) No. 1025/2012 as European standards adopted on the basis of a request made by the Commission for the application of Union harmonisation legislation. Once adopted by the standardisation organisation, the Commission shall assess the harmonised standards per Art. 36(10).

Art. 36(4) creates a presumption of conformity with the essential requirements prescribed by Art. 36(1) if the vendor of a smart contract can show compliance with the relevant parts of the harmonised standards. Unlike in the case of Art. 13(5), jointly read with rec. 62, this favourable presumption is arguably non-rebuttable.

Common Specifications (Art. 36(6) to (9))

Where the Commission's request under Art. 36(5) has not been accepted by the European standardisation organisation in question, or where the harmonised standards are not delivered within the applicable deadline or within the parameters of the request, the Commission may intervene in the absence of harmonised standards published in the Official Journal and adopt so-called common specifications. By this rather generic term, Art. 2(42) "means a document, other than a standard, containing technical solutions providing a means to comply with certain requirements and obligations established under [the Data Act]".

Rec. 103 is adamant to express the underpinning consideration that these common specifications "should be adopted only as an *exceptional fall-back solution* to facilitate compliance with the essential requirements of this Regulation" (emphasis added). The political struggle over who can claim the authority to determine essential requirements for smart contracts has thus been decided in favour of the European standardisation organisations.[532]

531 Annex I of Regulation (EU) No. 1025/2012.
532 Siglmüller, J., *MMR-Beil.* 2024, 112 (116).

With common specifications ranking below harmonised standards, the Commission must, in accordance with Art. 36(7), inform a dedicated committee under Art. 22 Regulation (EU) No. 1025/2012 before commencing the drafting process. Likewise, the Commission should first hear the advice of the EDIB, specifically of its sub-group on standardisation, interoperability, and portability.[533]

Like Art. 36(4), Art. 36(9) attributes to the common specifications a (non-rebuttable) presumption of conformity with the essential requirements for smart contracts. Unlike with harmonised standards, however, member states can notify the Commission that common specifications do not align with the essential requirements (Art. 36(11)).

8. Scope of Obligations

The scope of application of Chapter III is regulated in an unusual way at the end in Art. 12. The provisions apply accordingly where, in business-to-business-relations, a data holder is obliged under Art. 5, or under Union law or national legislation adopted in accordance with Union law, to make data available to a data recipient.[534]

According to Art. 12(2), an agreement that – to the detriment of a party or the user – derogated from the provisions of Chapter III is not binding in their respect. The rules of Art. 8-11 DA are therefore conceived as (partially unilateral) mandatory law.[535]

Art. 12 does not contain any statements on the relationship to the GDPR. To ensure the observance of the GDPR, one proposal was to add another paragraph that would have stated:

> "Any contractual term in a data sharing agreement between data holders and data recipients which, to the detriment of the data subjects undermines the application of their rights to privacy and data protection,

533 Established under Art. 29(2)(b) DGA; cf. Hennemann, M., in Specht-Riemenschneider, L. / id. (ed.), *Data Governance Act,* Nomos 2023, Art. 29 mn. 22.

534 The ITRE Draft Opinion proposed to add an Art. 12(1)(a) that would state: "The obligations set out in this Regulation do not preclude a reciprocity of data sharing between a data recipient, user and data holder agreed in contracts.", cf. ITRE PE739.548, p. 87.

535 Hennemann, M. / Steinrötter, B., *NJW* 2022, 1481 (1485).

> derogates from it, or varies its effect, shall not be binding on that party".[536]

However, the proposal was not included in the final version.

536 ITRE PE739.548, p. 88.