## V. Data Licence Agreement and User's Right of Access (Art. 4)

Fundamentally, the Data Act provides new access rights with respect to data generated by the use of a product of the user. Users may access data in the realm of the data holder and also request a sharing to third parties.[216] Conversely, limitations are placed on data holders and data recipients when it comes to the (secondary) use of the data.

### Definition of User and Data Holder

According to Art. 2(12) user means a natural or legal person that owns a connected product or to whom temporary rights to use that connected product have been contractually transferred, or that receives related services. Rec. 8 clarifies that users include data subjects.

Uncertainties in the definition of the draft Data Act whether the user is defined by the contractual relationship (lease, rent) or by an actual legal position (ownership)[217] were clarified by the final version's reference to "contractually transferred rights". Although the contractual transfer of a legal position is prerequisite for the application of Chapter II,[218] it remains an open question whether 'problems' within the contractual relation or with regard to the fulfilment of contractual obligations are relevant for the applicability of Chapter II. Examples include cases in which a void contract is nevertheless fulfilled or where a product is used after the termination of an underlying rental agreement.[219]

Rec. 18 additionally reads:

> "The user of a product should be understood as the legal or natural person, such as a business or consumer, but also a public sector body, that is either the owner of a connected product, or someone that has received certain temporary rights, for example by means of a rental

216 For further details cf. Hennemann, M. / Steinrötter, B., *NJW* 2022, 1481 (1483).
217 Bomhard, D. / Merkle, M., *RDi* 2022, 168 (170); Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 24 n. 59 et seq.; Cf. for a detailed discussion Specht-Riemenschneider, L., *MMR-Beil.* 2022, 809 (813 et seq.).
218 Schmidt-Kessel, M., *MMR-Beil.* 2024, 75 (77).
219 Schmidt-Kessel, M., *MMR-Beil.* 2024, 75 (77).

> or lease agreement, to access or use data obtained from the connected product, or that receives related services for the connected product. Those access rights should in no way alter or interfere with the rights of data subjects, who may be interacting with connected product or related service, to personal data generated by the connected product or during the provision of the related service. Such user bears the risks and enjoys the benefits of using the connected product and should enjoy also the access to the data it generates. The user should therefore be entitled to derive benefit from data generated by that product and any related service. An owner, renter or lessee should equally be considered as user, including when several entities can be considered as users. In the context of multiple users, each user may contribute in a different manner to the data generation and can have an interest in several forms of use, e.g. fleet management for a leasing company, or mobility solutions for individuals using a car sharing service."

While rec. 18 clarifies that multiple persons can be considered as users, it remains unclear how to deal with these scenarios where different persons are to be considered as users (e.g. owner, lessor, driver, regular driver etc. for a smart car).[220]

While the definition for "user" is relied upon at various points throughout the Data Act, it is used particularly often in the context of user-held access and sharing rights under Chapter II.

### Definition of Data Holder

According to Art. 2(13) data holder means a natural or legal person that has the right or obligation, in accordance with the Data Act, applicable Union law or national legislation adopted in accordance with Union law, to use and make available data, including, where contractually agreed, product data or related service data which it has retrieved or generated during the provision of a related service.

220 Cf. in this regard below sub IV. 1. and Bomhard, D. / Merkle, M., *RDi* 2022, 168 (170).

The definition "who has the right or obligation to make available data" is circular as according to Art. 4(1) the data holder is obliged to make data available.[221]

It is not clear whether the actual data access is a prerequisite for being a data holder. It is argued that not any obstacle in accessing the data should exclude the applicability of Art. 4-7.[222] The data holder might even evade the access obligations by deleting the data in question.[223] Consequently, it is partly argued that the user shall be notified before deletion and granted a possibility to access the data.[224]

Rec. 30 additionally points to the fact that users after having exercised its right to access might become a data holder themselves[225]:

> "It should be understood that such a user, once data has been made available, may in turn become a data holder, if they meet the criteria under this Regulation and thus become subject to the obligations to make data available under this Regulation."

Whereas the definition of "user" requires a contractually transferred legal position, the data holder is not necessarily the user's contractual partner. Nevertheless, the Art. 4-7 design the relation between data holder and user mainly as a contractual one.[226]

221 Cf. Bomhard/Merkle RDi 2022, 168 (169); Schmidt-Kessel, M., *MMR-Beil.* 2024, 75 (77).
222 Schmidt-Kessel, M., *MMR-Beil.* 2024, 75 (77).
223 Specht-Riemenschneider, L., *MMR-Beil.* 2022, 809 (815).
224 See Specht-Riemenschneider, L., *MMR-Beil. 2022*, 809 (815). Cf. also Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 25 n. 62.
225 In addition, data holder and user might be joint controllers according to Art. 26 GDPR, cf. rec 30.
226 Schmidt-Kessel, M., *MMR-Beil.* 2024, 75 (77).

### 1. Data Licence Agreement; Use by the Data Holder (Art. 4(13) and (14))

#### Data Licence Agreement

Art. 4(13) Sentence 1 is a true (but slightly hidden) 'revolution' introduced by the Data Act.[227] It limits the data holder's ability to use the data in question and empowers the user to market the data on his terms.[228]

The scope of the norm is limited to non-personal data (diverging from the general approach of the Data Act, but in order not to interfere with / to touch data protection law) that is 'readily available'. According to Art. 2(17) 'readily available data' "means product data and related service data that a data holder lawfully obtains or can lawfully obtain from the connected product or related service, without disproportionate effort going beyond a simple operation"; while 'product data' "means data generated by the use of a connected product that the manufacturer designed to be retrievable, via an electronic communications service, physical connection or on-device access, by a user, data holder or a third party, including, where relevant, the manufacturer" (Art. 2(15)). 'Related service data' refers to "data representing the digitisation of user actions or of events related to the connected product, recorded intentionally by the user or generated as a by-product of the user's action during the provision of a related service by the provider" (Art. 2 (16)).

The heavily debated and criticised[229] Art. 4(13) Sentence 1 stipulates that the data holder generally requires a contractual agreement with this user in order to use respective *non-personal* data. Rec. 25 confirms and adds:

> "This Regulation should not be understood to confer any new right on data holders to use product data or related service data. Where the manufacturer of a connected product is a data holder, the basis for the manufacturer to use non-personal data should be a contract between

227 Hennemann, M. / Steinrötter, B., *NJW* 2022, 1481 (1483) with further references. Cf. also Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 92: "crucial change".

228 Wiebe, A., *GRUR* 2023, 227.

229 E.g., Bomhard, D. / Merkle, M., *RDi* 2022, 168 (174); Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, pp. 92 et seq.; Max Planck Institute for Innovation and Competition, Position Statement, 2022, pp. 19 et seq. n. 45 et seq.; 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. 215 et seq.; Schweitzer, H. / Metzger, A., *GRUR-Int.* 2023, 337.

> the manufacturer and the user. Such a contract could be part of an agreement for the provision of the related service, which could be concluded together with the purchase, rent or lease agreement relating to the connected product."

The Data Act does not provide specific rules for the agreement according to Art. 4(13) (but see Art. 13).[230] Different follow-on problems result from this fact.[231] It is, for example, unclear under which conditions the data licence agreement may be terminated.[232]

The provision of Art. 4(13) raises further questions, for example with regard to the consequences of a rejection by a user or with regard to an amendment of the agreement.[233]

The user on the other hand can use the data for any lawful purpose (as rec. 30 confirms). It is another heavily debated question whether and in which setting users will actually negotiate and / or value the Art. 4(13)-agreement in practice.[234] There are strong concerns that the user will not be aware of the (additional) agreement which might even be concluded implicitly.[235] However, demands to combine Art. 4(13) with a 'bundling' prohibition to hinder a "Total-Buy-Out" were not integrated in the final Data Act.[236]

### Specific Limits of the Use of the Data Holder

According to Art. 4(13) Sentence 2 the data holder's use is limited in specific scenarios in which the data holder might "derive insights about the

230 Bomhard, D. / Merkle, M., *RDi* 2022, 168 (174).

231 Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 21 n. 52.

232 Hennemann, M. / Steinrötter, B., *NJW* 2022, 1481 (1484).

233 Krämer, J. et al. Data Act: Towards a balanced EU data regulation, CERRE report, March 2023, p. 41.

234 Strong doubts by Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 93; Specht-Riemenschneider, L., *MMR-Beil.* 2022, 809 (816 et seq.). Cf. also Podszun, R. / Pfeifer, C., *GRUR* 2022, 953 (956); Heinzke, P., *BB* 2023, 201 (208).

235 Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 93; Schwamberger, S., in Bernzen, A.K. / Grisse, K. / Kaesling, K. (ed.), Immaterialgüter und Medien im Binnenmarkt: Europäisierung des Rechts und ihre Grenzen, Nomos 2022, pp. 107 et seq.; Steinrötter, B., *GRUR* 2023, 216 (219).

236 Specht-Riemenschneider, L., *MMR-Beil.* 2022, 809 (817).

economic situation, assets and production methods of or the use by the user in any other manner that could undermine the commercial position of that user on the markets in which the user is active".

Rec. 27 points to cases that

> "involve using knowledge about the overall performance of a business or a farm in contractual negotiations with the user on potential acquisition of the user's products or agricultural produce to the user's detriment, or for instance, using such information to feed in larger databases on certain markets in the aggregate ([e].g. databases on crop yields for the upcoming harvesting season) as such use could affect the user negatively in an indirect manner."[237]

The wording "such data" indicates that Art. 4(13) Sentence 2 is referring to non-personal data covered by Art. 4(13) Sentence 1. Furthermore, having the different parallel norm of Art. 5(6) in mind, it is unclear whether the limitations set by Art. 4(13) Sentence 2 are subject to a disposal of the parties.[238]

Making data available to third parties

The data holders should not make non-personal data generated by the use of the product or related service available to third parties for any purposes other than the fulfilment of their contract with the user, Art. 4(14) sent 1. Data holders should also contractually bind third parties to not further share data received from them, Art. 4(14) sent. 2. This ensures that product or related service data is only made available to a third party at the request of the user (rec. 31) and solidifies the central position of the user.

It is however highly doubted whether this control of the user will foster the aim of the Data Act to enable independent innovation and competition in aftermarkets and complementary markets or if it will in fact hinder it massively.[239] Especially, where the user is a consumer, the effective availabil-

237 Rec. 25 further states that "[t]he user should be given the necessary technical interface to manage permissions, preferably with granular permission options (such as "allow once" or "allow while using this app or service"), including the option to withdraw permission."

238 Hennemann, M. / Steinrötter, B., *NJW* 2022, 1481 (1484).

239 Schweitzer, H./Metzger, A., *GRUR Int.* 2023, 337; Kerber, W., Towards a dynamic concept of competition that includes innovation, OECD 2023, 42, p. 17.

ity of the data on the market is questionable. However, the user is free to market the data, including to give the right to market the data contractually to a third party, such as data intermediation services according to the Data Governance Act.[240]

### De facto-Control by Agreement?

The requirement of a data licence agreement does not depend on the right to access (and use) according to Art. 4(1) – or its exercise. Rather this requirement of an agreement has the severe consequence that the data holder may not process non-personal data without a respective contractual agreement. This is a 'revolution' with regard to non-personal data.[241] Art. 4(13) and Art. 4(14) lead to the surprising result that the processing of non-personal data is subject to stricter rules than the processing of personal data.[242] However, it has also been questioned whether this will have actual impact in practice.[243] On the one hand, concerning the data licence agreement a "Total-Buy-Out" is possible,[244] on the other hand Art. 4(14) additionally limits the data holder's possibility to make the data available to third parties regardless of the data licence agreement. So, while the actual control over the use of data given to users by Art. 4(13) depends on their bargaining power,[245] Art. 4(14) clearly empowers the user to control the making available of non-personal data. This shows that the Data Act follows a different concept compared to the GDPR, as it is not about the

240 Cf. Hennemann, M./ Steinrötter, B., *NJW* 2024, 1 (7).

241 Henneman, M. / Steinrötter, B., NJW 2022, 1481(1483).

242 Bomhard, D. / Merkle, M., RDi 2022, 168 (174); Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 20 n. 49; Schweitzer, H. / Metzger, A. / Blind, K. /Richter, H. / Niebel, C./ Gutman, F.; The legal framework for access to Data in Germany and in the EU, BMWK, 2022, p. 216; Specht-Riemenschneider, L., MMR 2022, 809 (816).

243 Schwamberger, S., Der Datenzugang im Data Act: Fortschritt oder Rückschritt?, in: Bernzen, A. K. et al., Immaterialgüter und Medien im Binnenmarkt, Nomos 2022, 88 (107 et seq.); Steinrötter, B., GRUR 2023, 2016 (219).

244 Schwamberger, S., Der Datenzugang im Data Act: Fortschritt oder Rückschritt?, in: Bernzen, A. K. et al., Immaterialgüter und Medien im Binnenmarkt, Nomos 2022, 88 (107 et seq.); Steinrötter, B., GRUR 2023, 2016 (219).

245 Grapentin, S., *RDi* 2023, 173 (179); Krämer, J. et al. Data Act: Towards a balanced EU data regulation, CERRE report, March 2023, p. 41.

protection of data but about the control over the use and making available of data.[246]

As the data licence agreement leads to a control option for the user, it could be seen as (contractually) attributing the right to use and share non-personal data to the user.[247] Otherwise, some understand the access regulation of the Data Act as a manifestation of the technical-factual 'rule' of the data holder who 'only' might have to grant access to data 'under his control'.[248] To the same end, others emphasise the co-generation of data by the data holder and the user.[249] Some commentators associate such a co-generation with the idea of a 'co-property' (Miteigentum) leading to a general 'right' of both the data holder and the user to use the respective non-personal data.[250]

It is generally – and beyond Art. 4(13) – heavily debated whether and to what extent the data access regime introduces and / or paves the way for some type of 'absolute' / 'IP-like' right regarding non-personal data.[251] This debate has to be seen against the background that on the basis of the current law non-personal data (if one has access and notwithstanding trade secret law) can be used freely and without some form of consent and / or agreement by the 'producer'.

Understanding the rights conferred to the user as "absolute" is contradicted by the fact that they only apply in relation to the data holder and that

246 Wienroeder, M., PinG 2024, 103 (106).

247 Cf. also Bomhard, D. / Merkle, M., RDi 2022, 168 (174); Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 19 n. 45.

248 Kerber, W., Governance of IoT Data: Why the EU Data Act Will not Fulfill Ist Objectives, 2022, https://doi.org/10.1093/grurint/ikac107, p.p. 5et seq.; Specht-Riemenschneider, L., MMR 2022, 809 (818). Cf. Also the proposal of a new Art. 4(4a) by Council Presidency 2022/0047 (COD) – 15035/22, p. 44 in this regard.

249 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, p. 219; Metzger, A. / Schweitzer, H., ZEuP 2023, 42; as well as Leistner, M. / Antoine, L.; IPR and the use of open data and data sharing initiatives by public and private actors, 2022, pp. 85 et seq., 93 et seq.

250 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, p. 216; Metzger, A. / Schweitzer, H., ZEuP 2023, 42; as well as Leistner, M. / Antoine, L.; IPR and the use of open data and data sharing initiatives by public and private actors, 2022, pp. 80.

251 See in detail Max Planck Institute for Innovation and Competition, Position Statement, 2022, pp. 19 et seq. n. 44 et seq.

the attribution of rights is completely contractual.[252] Furthermore Art. 4(14) sent. 2 would not be necessary if the user had an absolute right.[253]

Despite the fact that the Data Act does not introduce any 'absolute' rights, this attribution of control to the user requires a careful evaluation – also with regard to its economic consequences.[254]

It is questioned whether this control option of the user in relation to the data holder is justified. It is pointed to the fact that the 'generation' of data takes regularly place incidentally and is not connected to any specific efforts of the user.[255] Thus, the 'co-generation' of data serves as the reason that both user and data holder should be able to use the data without the approval of the other party but cannot justify the control-option of the user.[256] Others argue that it is compatible with the general legislative approach which gives the right to use a product and its advantages to the buyer or lessee.[257]

### Unfair Terms Control

A data licence agreement is generally subject to the unfair terms control according to Art. 13. This is justified as in some scenarios the user might even have more bargaining power than the data holder and may be in the position to 'dictate' the conditions of the licence agreement.[258] However, Art. 13 does only apply to business-to-business scenarios.[259]

However, rec. 25 might be regarded as a "minimum line" in this regard (also in b2c-scenarios). Rec. 25 combines in a rather confusing way elements of Art. 3(2)[260] and substantial elements:

> "Any contractual term in the agreement stipulating that the data holder may use the data generated by the user of a product or related service should be transparent to the user, including as regards the purpose for

252 Cf. Heinzke, P., BB 2023, 201 (207 et seq.); Schmidt-Kessel, M., MMR-Beil. 1/2024, 75 (78).
253 Schmidt-Kessel, M., MMR-Beil. 1/2024, 75 (78).
254 Hennemann, M. / Steinrötter, B., NJW 2022, 1481 (1486).
255 Funk, A., CR 2023, 421 (425).
256 Cf. Metzger, A. / Schweitzer, H., ZEuP 2023, 42 (54 et seqq.).
257 Schmidt-Kessel, M., MMR-Beil. 1/2024, 75.
258 Grapentin, S., *RDi* 2023, 173 (179); Krämer, J. et al. Data Act: Towards a balanced EU data regulation, CERRE report, March 2023, p. 41.
259 See below VII.
260 See above IV. 3.

> which the data holder intends to use the data. (...) This Regulation should not prevent contractual conditions, whose effect is to exclude or limit the use of the data, or certain categories thereof, by the data holder."

### *2. The Right to Access according to Art. 4(1))*

#### Economic Setting and Assumptions

Art. 4(1) stipulates the Act's key instrument to the benefit of the user, a statutory right to get access to readily available data (along with the relevant set of metadata that is necessary to interpret and use those data). Recognising that these data are "an important input for aftermarket, ancillary, and other services" (rec. 6), the legislator hopes to unlock data silos hitherto controlled exclusively by the data holder and to decrease transaction costs in data-rich markets.[261]

Rec. 15 underlines:

> "[Respective] data are potentially valuable to the user and support innovation and the development of digital and other services protecting the environment, health and the circular economy, in particular though facilitating the maintenance and repair of the products in question."[262]

From a Law & Economics perspective, the data access right introduced by Art. 4(1) has been the subject of intense scrutiny. It is highly debated whether and to what extent the right sets functionally calibrated, sensible, and thought-through parameters and incentives.[263] Whilst there seems to be a general consensus that an information-only / transparency-only approach (cf. Art. 3(2)) would have been insufficient[264], it was and is variously argued that the construction of the right does not go far enough to achieve the stated goals and fulfil the aforementioned aspirations.

---

261 Paal, B. / Fenik, M., ZfDR 2023, 249 (253 et seq.); Heinzke, P., *BB* 2023, 201 (203).

262 This phrase had first been suggested by Council Presidency 2022/0047(COD) – 15035/22, p. 11.

263 Cf. in this regard Kerber, W., *GRUR Int.* 2023, 120 (128); Krämer, J., Improving The Economic Effectiveness of the B2B and B2C Data Sharing Obligations in the Proposed Data Act, CERRE, 2022; 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, p. 212.

264 Cf. Krämer, J., Improving The Economic Effectiveness of the B2B and B2C Data Sharing Obligations in the Proposed Data Act, CERRE, 2022, p. 10.

The criticism pertains, first, to which kind of data shall be made accessible, and especially takes issue with the exclusion of derived or inferred data as well those datasets aggregated from multiple sensors and data points.[265]

Second, commentators point out that the user's claim to data access does not alter the technical 'rule' of the data holder, who still might be the only one being able to access the respective product in a *de facto* sense.[266] For instance, Art. 4(11) presupposes that the technical infrastructure storing and variously processing the data at issue is not currently accessible to the user, whereas rec. 22 accepts a computing instance of the manufacturer (i.e., data holder) as a viable gateway for access.

In opposition of the one size fits all-framework constructed by the Act, sectoral approaches have been put forth as an alternative.[267] Similarly, a general set of rules for b2b and b2c scenarios alike is not considered the appropriate regulatory course of action.[268]

Other critiques turn to the user-centricity of the access right[269] and discuss whether collecting data sets from every user individually and not receiving bulk data is economically feasible and / or sensible – also with regard to SMEs.[270] Significant doubts are cast on the practical success of the user activation upon which the access right rests at a foundational level.[271]

265 Cf. in this regard Krämer, J., Improving The Economic Effectiveness of the B2B and B2C Data Sharing Obligations in the Proposed Data Act, CERRE, 2022, pp. 12 et seq.; Max Planck Institute for Innovation and Competition, Position Statement, 2022, pp. 10 et seq. n. 20 et seq.

266 *Ex multis*, Finck, M. / Mueller, M-S., 35 (2023) *Journal of Environmental Law* 109 (125).

267 Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 3 n. 3.

268 Kerber, W., *GRUR-Int.* 2023, 120 (134).

269 Dismissed as a useful premise by Funk, A., *CR* 2023, 421 (425 et seq.).

270 Cf. Krämer, J., Improving The Economic Effectiveness of the B2B and B2C Data Sharing Obligations in the Proposed Data Act, CERRE, 2022, p. 20 as well as Bomhard, D. / Merkle, M., *RDi* 2022, 168 (173); Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, pp. 78, 100 et seq.; Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 9 n. 19.

271 Cf. e.g., Podszun, R. / Pfeifer, C., *GRUR* 2022, 953 (956).

### A Remedy for Lack of Data Accessibility-by-Design under Art. 3(1)

Apart from its debatable (behavioural and competition) economic foundations, the right of access raises doctrinal questions. Perhaps the most important one concerns the interplay with the accessibility-by-design[272] demand of Art. 3(1) – both provisions being geared towards the relationship between user and data holder as well as to readily available data.[273]

Access rights seem to be superfluous where the user can access the data sets in question for themselves without further ado[274], but the issue is complicated by vague statutory wording. Namely, under Art. 4(1) the right's availability is conditional upon a situation "[w]here data cannot be directly accessed by the user from the connected product or related service", thus giving precedence to Art. 3(1).[275] Direct accessibility in the way of network access to on-device data storage or via a remote server (cf. rec. 22) is subject to the decisive *caveat* that such access mechanisms must turn out as "relevant and technically feasible". The dual requirement of relevance and technical feasibility (re-appearing in Art. 4(1) and Art. 5(1)) is not explained by the legislator and hence remains woefully unclear.[276] Ultimately, this could become a matter for evaluation of the Act under Art. 49(1)(c).

Manufacturers failing to make product data and related services data directly accessible in violation of Art. 3(1) is the second scenario that will trigger the access right.[277] *Schmidt-Kessel* argues that, in this case, manufacturers as data holders are barred from invoking defences under Art. 4 (notably, regarding trade secrets) as they could otherwise circumvent

272 Despite Art. 3(1) being phrased in the latter way, the label "accessibility by design" more precisely captures the technicalities of product design when compared to "access by default"; both terms could also be linked, cf. Paal, B. / Fenik, M., *ZfDR* 2023, 249 (255).

273 Schwamberger, S., in Bernzen, A. K. / Grisse, K. / Kaesling, K. (ed.), Immaterialgüter und Medien im Binnenmarkt: Europäisierung des Rechts und ihre Grenzen, Nomos 2022, p. 101.

274 Specht-Riemenschneider, L., *MMR-Beil.* 2022, 809 (815); Heinzke, P., *BB* 2023, 201 (207).

275 Schmidt-Kessel, M., *MMR-Beil.* 2024, 75 (79).

276 Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 30 n. 73; Specht-Riemenschneider, *MMR-Beil.* 2022, 809 (815); Podszun, R. / Pfeifer, C., *GRUR* 2022, 953 (956) (opining - with reference to the initial Commission Proposal - that criteria for judging the relevance and appropriateness of direct accessibility should be easy to develop); further, cf. sub IV.2.

277 Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 32 n. 79; Specht-Riemenschneider, *MMR-Beil.* 2022, 809 (815).

Art. 3(1) to their benefit. This viewpoint can mainly draw on the initial part of Art. 4(1) and the underlying "remedial" nature of the right to access, ensuring specific performance of access to data where accessibility-by-design is lacking.[278]

### Effect of the Right: In-Situ Access, Data Retrieval and / or Usage?

Rec. 30 stipulates:

> "The user should be free to use the data for any lawful purpose. This includes providing the data the user has received exercising the right under this Regulation to a third party offering an aftermarket service that may be in competition with a service provided by a data holder, or to instruct the data holder to do so."

In terms of when data sets have been received by, that is made "accessible to the user"[279] pursuant to Art. 4(1), the debate spills over from Art. 3(1)[280]. Can the data holder resort to granting "simple access"[281], i.e. by only allowing processing of (or even less invasive, read-only access to) the data on infrastructure it controls (*in situ*)? Independently from one another, rec. 8 and rec. 22 raise a strong inference that such *in-situ* access could be sufficient:[282]

> "Taking into account the state of the art, all parties to data sharing, including data sharing falling within scope of this Regulation, should implement technical and organisational measures to protect those rights. Such measures include not only pseudonymisation and encryption, but also the use of increasingly available technology that permits algorithms to be brought to the data and allow valuable insights to be derived

278 Schmidt-Kessel, M., *MMR-Beil.* 2024, 75 (80).

279 Further ambiguities between Art. 3(1) and Art. 4(1) are found in the German-language version (*Zugriff* vs. *Zugang*); cf. Podszun, R. / Pfeifer, C., *GRUR* 2022, 953 (957).

280 Cf. sub IV.2.

281 ALI-ELI Principles for a Data Economy, Pr. 8 cmt. a coin this term (as opposed to transfers); cf. Schwamberger, S., in Bernzen, A. K. / Grisse, K. / Kaesling, K. (ed.), Immaterialgüter und Medien im Binnenmarkt: Europäisierung des Rechts und ihre Grenzen, Nomos 2022, p. 105 n. 69.

282 In detail: Kerber, W., *GRUR-Int.* 2023, 120 (124); with respect to rec. 22, cf. also Specht-Riemenschneider, L., *MMR-Beil.* 2022, 809 (816).

> *without the transmission between parties or unnecessary copying of the raw or structured data themselves.*" (rec. 8, emphasis added)

> "Connected products may be designed to permit the user or a third party to process the data on the connected product, *on a computing instance of the manufacturer* or within an information and communications technology (ICT) environment chosen by the user or the third party." (rec. 22, emphasis added)

Upon closer analysis, rec. 8 does not specifically address the right under Art. 4(1) but touches upon adjacent matters. *In-situ* access is recommended[283] (not: mandated) as a technical protection measure in the context of Art. 11, chiefly to prevent unauthorised access and to operationalise the requirements of Art. 4 et seq.[284] In the same breath, Art. 11(1) prescribes limitations to technical protection measures taken by the data holder which "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 (...)". By eliminating the reference to Art. 5, the power to "obtain a copy of, retrieve, use or access data" has to be seen as describing the varied contents of the right granted by Art. 4(1), thereby surpassing mere *in-situ* access.

In contrast, the wording of rec. 22 covers the access regime from Art. 3(1) through to Art. 5(1) ("user or a third party").[285] Given that the notion of processing is mentioned here, rec. 22 can however not be construed to advocate for read-only access as the mere inspection of the data in question does not amount to an operation performed on them (Art. 2(7); cf. Art. 4(2) GDPR).[286] The assumption of a data holder's discretion to simply allow for processing *in situ* without having to migrate the data is refuted by a contextual interpretation of Art. 4(1). For example, the prohibition on ensuing usage in Art. 4(10) only becomes significant if the user is allowed to download or otherwise retrieve the data while observing Art. 4(11).[287] More generally, sole *in-situ* access would run afoul of the Act's broader objectives

283 Kerber, W., *GRUR-Int.* 2023, 120 (124).
284 On the exclusionary relationship between Art. 11 and Art. 3(1), cf. Steege, H., *MMR-Beil.* 2024, 91 (92) and the section devoted in this work to Art. 11 (VI.6.).
285 Specht-Riemenschneider, L., *ZEuP* 2023, 638 (669).
286 Steinrötter, B., *GRUR* 2023, 216 (222); in apparent disagreement: Specht-Riemenschneider, L., *ZEuP* 2023, 638 (669).
287 Correctly, Steinrötter, B., *GRUR* 2023, 216 (222).

to break up data silos and let users share in on the economic benefits of data generation (cf., e.g., rec. 2 and rec. 6).[288]

Ultimately, Art. 4(1) should be understood as implying data retrieval *ex situ*, not least because rec. 22 factors in an ICT environment *chosen by the user* as a viable gateway for access. Structurally, the right then draws inspiration from the right to indirect personal data portability pursuant to Art. 20(1) GDPR – despite key differences in scope (cf. rec. 35).[289] This conclusion does not remove *in-situ* access entirely from consideration, but might relegate it to a defence where data transfers would compromise the confidentiality of trade secrets.[290] In some cases, *in-situ* access may also be preferred by users from a data protection and security viewpoint.[291]

### Mandatory Nature of Art. 4; No Circumvention through 'Dark Patterns' (Art. 4(4))

As it is the case with other user rights of Chapter II, Art. 7(2) codifies the semi-mandatory[292] nature of the right to access. Private-law arrangements may not derogate from, let alone contract away the conditions or effects of the right to the detriment of the user. Importantly, this is not to deny the data holder's varied statutory defences pursuant to Art. 4(2), (7), (8), and (11) (which are analysed in-depth in the following section).

The semi-mandatory conception has seen criticism from *inter alia* an Economics perspective.[293] Introducing an element of waivability may however risk defeating the very goals of the Act's data access regime, namely to

288 Heinzke, P., *BB* 2023, 201 (206); Schwamberger, S., in Bernzen, A. K. / Grisse, K. / Kaesling, K. (ed.), Immaterialgüter und Medien im Binnenmarkt: Europäisierung des Rechts und ihre Grenzen, Nomos 2022, p. 105.

289 Concurringly, Geiregat, S., 'The Data Act: Start of a New Era for Data Ownership?' 2022, p. 21 at para. 20 ("conceptual likeness"); Richter, S., *MMR* 2023, 163 (165); Callewaert, C., Data Act und Datenportabilität - Lesson Learned?, in Heinze, C. (ed.), Daten, Plattformen und KI als Dreiklang unserer Zeit, DSRI, 2022, p. 422; Steinrötter, B., *GRUR* 2023, 216 (220-221) agrees in principle, but – supported by Art. 1(5) – also points out a close resemblance to Art. 15(3) GDPR.

290 Paal, B. / Fenik, M., *ZfDR* 2023, 249 (261).

291 Hennemann, M. / Steinrötter, B., *NJW* 2024, 1 (3).

292 Schmidt-Kessel, M., *MMR-Beil.* 2024, 75 (77).

293 E.g., by 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, p. 219.

counteract data silos and to enable competition in aftermarkets.[294] Instead, a (time-limited) revocable waiver has been favoured both to incentivise long-term investments by a data holder exploiting a data resource exclusively and to allow users to participate *ex post* in previously unforeseen value creation with product and related services data.[295]

It is worth recalling that the non-waivability of the access right does not extend to the use of the data after obtaining access. In line with Art. 4(13), the data licensing agreement concluded between the data holder and the user may provide for a "Total Buy-Out" clause.[296] Rec. 25 bears this in mind for b2b constellations, stating that "[the Act] does not prevent users, in the case of business-to-business relations, [...] from being compensated proportionately, for example in exchange for waiving their right to use or share such data."

On a related note, Art. 4(4) is best understood as preventing circumvention of and manipulation away from the mandatory access right, chiefly in b2c-contexts. According to this provision, "data holders shall not make the exercise of choices or rights under [Art. 4] by the user unduly difficult, including by offering choices to the user in a non-neutral manner or by subverting or impairing the autonomy, decision-making or choices of the user via the structure, design, function or manner of operation of a user digital interface or a part thereof".[297] As rec. 38 clarifies, so-called 'dark patterns' in the design of digital interfaces – defined as "design techniques that push consumers or deceive consumers into decisions that have negative consequences for them" – are outlawed as a result. Rec. 38 further mentions (manipulative) persuasion, nudging, and introducing bias to the decision-making of users as examples. *Martini et al.* interpret this approach to cover well-known design techniques like nagging, forced enrolment, misdirection, obstruction, and bait and switch.[298] Other recently enacted bans on dark patterns found in Art. 5, Art. 13(6) DMA, Art. 25 DSA, as

294 Schweitzer, H. / Metzger, A., 'Shaping Markets: A Critical Evaluation of the Draft Data Act', *ZEuP* 2023, 42 (57); Paal, B. / Fenik, M., *ZfDR* 2023, 249 (259).
295 In-depth Schweitzer, H. / Metzger, A., *ZEuP* 2023, 42 (56 et seqq.).
296 See the discussion sub V.1. above; additionally, cf. Kerber, W., *GRUR-Int.* 2023, 120 (132); Specht-Riemenschneider, L., *MMR-Beil.* 2022, 809 (817); Steinrötter, B., *GRUR* 2023, 216 (219).
297 First proposed by Council Presidency 2022/0047(COD) – 15035/22, p. 44.
298 Martini, M. / Kramme, I. / Kamke, A., *MMR* 2023, 399 (401 et seq.).

well as in Art. 5(1)(a) of the AI Act[299], tend to be more comprehensive and extend to further instances of dark patterns.[300]

### Modalities under which Access is Granted as per Art. 4(1)

Once the access right is deemed applicable, the modalities of how and when data sets have to be made accessible come into play. Art. 4(1) lists extensive requirements, namely that access has to be granted "without undue delay, of the same quality as is available to the data holder, easily, securely, free of charge, in a comprehensive, structured, commonly used and machine-readable format and, where relevant and technically feasible, continuously and in real-time."[301]

What qualifies as 'undue delay' is determined by Union, not by member state law.[302] The same language in Art. 12(3) GDPR is interpreted as the shortest amount of time needed to supply the requested data.[303] Taken to the extreme, this could coincide with real-time access under Art. 4(1) and hence be a matter of mere seconds.[304] It should be pointed out that in contrast, Art. 12(3) GDPR sets the maximum time frame at one month (possibly lengthened by another two months). In case personal data is concerned, frictions between Art. 20 GDPR and Art. 4(1) as well as Art. 5(1) will result, the resolution of which may depend on the declared intent of the data subject / user.[305]

Similar frictions are bound to arise where data subjects as users submit overly repetitive requests, i.e. those exceeding reasonable intervals.[306]

299 European Parliament legislative resolution of 13 March 2024 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts, p. 181.

300 Martini, M. / Kramme, I. / Kamke, A., *MMR* 2023, 399 (399 et seq.).

301 Most of these requirements stem from Council Presidency 2022/0047(COD) – 15035/22, p. 44 – also tackling criticism of the original proposal of Art. 4(1), cf. e.g., Krämer, J., Improving The Economic Effectiveness of the B2B and B2C Data Sharing Obligations in the Proposed Data Act, CERRE, 2022, p. 7.

302 Schmidt-Kessel, M., *MMR-Beil.* 2024, 75 (79).

303 EDPB, 'Guidelines 01/2022 on data subject rights - Right of access', 28 March 2023, p. 50 n. 158.

304 Hartmann, B. / McGuire, M. / Schulte-Nölke, H., *RDi* 2023, 49 (53).

305 Richter, S., *MMR* 2023, 163 (166).

306 Rec. 63 GDPR with guidance by EDPB, 'Guidelines 01/2022 on data subject rights - Right of access', 28 March 2023, p. 56 n. 183 et seq.

Whereas access remains 'free of charge' under Art. 4(1), the data holder (viz. controller) could charge for access and indirect portability pursuant to Art. 12(5) GDPR.[307] Making access 'free of charge' does not prohibit data holders from pricing in the related costs as service fees.[308] According to rec. 28, it does however preclude tying access to unfair contractual terms within the meaning of Directives 93/13/EEC and 2005/29/EC where the user is a consumer. Rec. 28 extends this to b2b scenarios involving enterprises (cf. Art. 2(24)) as users, rendering such terms unenforceable across the board.[309]

Turning to the option of *continuous and in real time access*, the already familiar hurdle of relevance and technical feasibility must be cleared, which should be the case where the connected product actually stores data on end and in real time.[310] In practice, data holders will invoke this exception by discharging their notice obligation pursuant to Art. 3(2)(b). Continuous and real-time data transfers represent perhaps the most significant advance over one-off (*ad hoc*) downloads in the context of Art. 20(1) GDPR since they best capture the value of data stemming from its immediate availability.[311] What is more, the technical tools necessary to enable real-time access, namely application programming interfaces (APIs), will be conducive to interoperability.[312] The like-minded rule targeting participants in data spaces (Art. 33(1)(c)), which alludes to connected products, should be read as part of the requirements under Art. 4(1).[313]

As for the *quality* in which data has to be made accessible, it is not unheard of that data holders unwilling to share certain datasets will deliber-

307 Steinrötter, B., *GRUR* 2023, 216 (221).

308 As is noted by Funk, A. *CR* 2023, 421 (426).

309 It stands to reason that unfair terms would also materially alter and therefore derogate from the user's access right in contravention of Art. 7(2) (as reiterated towards the end of Art. 8(2)).

310 Geiregat, S., 'The Data Act: Start of a New Era for Data Ownership?' 2022, p. 21 at para. 21.

311 Krämer, J., Improving The Economic Effectiveness of the B2B and B2C Data Sharing Obligations in the Proposed Data Act, CERRE, 2022, p. 7; Schwamberger, S., in Bernzen, A. K. / Grisse, K. / Kaesling, K. (ed.), Immaterialgüter und Medien im Binnenmarkt: Europäisierung des Rechts und ihre Grenzen, Nomos 2022, p. 94.

312 Krämer, J., Improving The Economic Effectiveness of the B2B and B2C Data Sharing Obligations in the Proposed Data Act, CERRE, 2022, p. 7; further, cf. sub IX.9.

313 To that effect: Schweitzer, H. / Metzger, A., *ZEuP* 2023, 42 (72); cf. sub IX.10.

ately degrade their – otherwise constant – quality.[314] Reinforced by unfair terms control for unilaterally imposed standards of data quality pursuant to Art. 13(5)(g)[315], Art. 4(1) makes sure that the quality does not dip below the level available to the data holder. Rec. 30 expands on which criteria pertain to this assessment:

> "Data holders should ensure that the data made available to the third party is as accurate, complete, reliable, relevant and up-to-date[316] as the data the data holder itself may be able or entitled to access from the use of the connected product or related service."

Rec. 30 mistakenly refers only to "data made available to the third party". From the positioning and content of rec. 30 on the whole, however, it can be deduced that the elements of data quality mentioned also apply to the access of the user as such.

The obligation to maintain data quality is likewise placed under the *caveat* of relevance and technical feasibility, the reason being that the individual needs of a user may call for a different presentation of the data at issue.[317]

Following suggestions from academia[318], the requirements of a *structured, commonly used, and machine-readable format* are lifted verbatim from Art. 20(1) GDPR. Yet in doing so, the well-known uncertainties of this phrase are reproduced. According to (inconclusive) guidance, the term "structured" should be interpreted with a view to how easily the data can be re-used at the destination[319], which would likely exclude PDF and HTML files in IoT contexts.[320] The notion of machine-readability is susceptible to

314 Krämer, J., Improving The Economic Effectiveness of the B2B and B2C Data Sharing Obligations in the Proposed Data Act, CERRE, 2022, p. 19; cf. Paal, B. / Fenik, M., *ZfDR* 2023, 249 (253).

315 Cf. sub VII, below.

316 Similarly, Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 43 n. 116; for a different view of which factors make up data quality, cf. von Lewinski, K. / Hähnle, J., *DuD* 2021, 686 (687) (adding usability and presentation quality / readability).

317 Schmidt-Kessel, M., *MMR-Beil.* 2024, 75 (80).

318 E.g., by Schweitzer, H. / Metzger, A., *ZEuP* 2023, 42 (72).

319 Article 29 Working Party, 'Guidelines on the right to data portability' WP 242 rev.01 (5 April 2017) p. 18.

320 Cf. Dix, A., 'DSGVO Art. 20 Recht auf Datenübertragbarkeit', in Simitis, S. / Hornung, G. / Spiecker gen. Döhmann, I. (ed.), Datenschutzrecht: DSGVO mit BDSG, Nomos 2019, para. 11.

wildly diverging interpretations, from OCR-readable paper formats on one end[321] to autonomously machine-readable formats on the other (thereby excluding most text- and image-based files).[322] A format is commonly used where it is widely accepted in the relevant market, with open formats such as XML, JSON, and CSV being recommended in the context of Art. 20 GDPR.[323] The additional insistence on a *comprehensive* format prohibits the data holder from relying, to the detriment of users, on a blend of multiple formats for the same access request.

### Data in Scope of the Access Right

Per Art. 4(1), "readily available data, as well as the relevant metadata necessary to interpret and use those data" has to be made accessible to the user. Because Art. 2(17) defines 'readily available data' as the umbrella term for product data and related service data, Art. 4(1) uses practically the same language as Art. 3(1). Logically sound, the scope of the data coming within the access right corresponds to the extent of accessibility-by-design. In particular, inferred and derived data are excluded (rec. 15).[324] From a different angle, the breadth of data covered under the right goes as far as is permissible in accordance with data protection law.[325] Rec. 35 highlights how the user-held access right thereby seeks to improve upon Art. 20(1) GDPR (apart from the aforementioned continuous and real-time access):

> "This Regulation grants users the right to access and make available to a third party any product data or related service data, irrespective of their nature as personal data, of the distinction between actively provided or passively observed data, and irrespective of the legal basis of processing."

321 Hennemann, M., *PinG* 2017, 5 (7).
322 Geiregat, S., 'The Data Act: Start of a New Era for Data Ownership?' 2022, p. 36 at para. 36.
323 Article 29 Working Party, 'Guidelines on the right to data portability' WP 242 rev.01 (5 April 2017) p. 18; for JSON and fitness tracking apps, this has recently been affirmed in a decision by the Austrian Federal Administrative Court (ECLI:AT:BVWG:2023:W211.2261980.1.00 at para 3.3.2).
324 Cf. IV.2 and the beginning of this section.
325 Bomhard, D. / Merkle, M., *RDi* 2022, 168 (169).

Identification of the Requesting User (Art. 4(5))

According to its second sentence, the right under Art. 4(1) is exercised via "a simple request through electronic means where technically feasible". Rec. 29 adds that "[i]n the case of personal data processed by a processor on behalf of the controller, data holders should ensure that the access request is received and handled by the processor."

The user does not have to observe a specific form and can submit the request at any given time.[326] Delaying the access request is not advisable however because data holders are not expected, let alone required to store the data generated by connected products indefinitely. Instead, rec. 24 vaguely stipulates that a reasonable data retention policy must be implemented by the data holder (balancing storage limitation under Art. 5(1)(e) GDPR and the effectiveness of access rights). While immediate deletion upon generation would clearly violate accessibility-by-design (Art. 3(1))[327], data holders may subsequently choose to rid themselves of data sets they have already analysed – along with the associated obligations under Art. 4 et seq.[328] No matter how long data is being retained, the duration must be communicated to the user under Art. 3(2)(c) and Art. 3(3)(a)-(b) in order not to undermine the concept of access upon request.[329]

Art. 4(5) tackles the question of how data holders know whether the 'correct' user is requesting access. By limiting the data holder to information that is necessary to verify the user, the principles of purpose limitation and data minimisation as per Art. 5(1)(b) and (c) GDPR are unnecessarily duplicated.[330]

No information on the requested access shall be kept that is not "necessary for the sound execution of the user's access request and for the security and the maintenance of the data infrastructure" (Art. 4(5) Sentence 2). Not least by singling out log data (recording changes to and retrieval of elements in a database[331]), it becomes apparent that the legislator intended for the user and for third parties to use the data without being obliged

326 Specht-Riemenschneider, L., *MMR-Beil.* 2022, 809 (815); Heinzke, P., *BB* 2023, 201 (206).
327 Schweitzer, H. / Metzger, A., *ZEuP* 2023, 42 (52).
328 Bomhard, D. / Merkle, M., *RDi* 2022, 168 (174).
329 Further, cf. IV.3, above.
330 Hennemann, M. / Steinrötter, B., *NJW* 2024, 1 (3).
331 Butterfield, A. / Ngondi, G.E. / Kerr, A. (ed.), A Dictionary of Computer Science, s.v. "log file", 7th edn, OUP 2016.

to reveal to the data holder their (competitively relevant) business plans with regard to specific data sets.[332] As rec. 21 puts it, no "examination or clearance [of the request] by the manufacturer or data holder" should be needed.

Additionally, rec. 21 concedes (and does not attempt to change) the fact that use of a connected product or related service will typically entail setting up a user account. This has been criticised as effectively barring anonymous usage of IoT products, including access requests.[333]

### *3. Limitations of and Defences to the User's Right of Access*

The remaining parts of Art. 4 turn to the interests of data holders in two ways: first, by establishing defences[334] against the user's access right concerning matters of cybersecurity (Art. 4(2)), confidentiality of trade secrets (Art. 4(6)-(9)), and data protection (Art. 4(12)); and second, by establishing loyalty obligations of users[335] towards data holders in accordance with Art. 4(10)-(11).

#### No 'Right to Hack'[336] (Art. 4(11))

Even prior to access, Art. 4(11) articulates a duty of loyalty in denying users a 'right to hack'. Coercive means may not be used, gaps in the technical infrastructure may not be abused (even if they are widely known). The user accordingly cannot 'self-remedy' refusals or delays on the part of the data holder and take the access 'into their own hands' by penetrating the IoT-product through exploits not foreseen / enabled by the data holder. Art. 4(11) is considered as tightening the previously discussed *de facto* technical control attributed to the data holder.[337]

---

332 Schweitzer, H. / Metzger, A., *ZEuP* 2023, 42 (55).
333 Podszun, R. / Pfeifer, C., *GRUR* 2022, 953 (961); Specht-Riemenschneider, L., *ZEuP* 2023, 638 (663 et seq.).
334 Cf. Hennemann, M. / Steinrötter, B., *NJW* 2024, 1 (4).
335 Schmidt-Kessel, M., *MMR-Beil.* 2024, 75 (81) ("*Schutz- und Treuepflichten*").
336 Specht-Riemenschneider, L., *MMR-Beil.* 2022, 809 (823) (with regard to the parallel norm in Art. 5(5)).
337 Kerber, W., *GRUR-Int.* 2023, 120 (124 et seq.); cf. sub 2.

### Security of the Connected Product (Art. 4(2))

It is possible to restrict access to, (further) use or sharing of the data at the outset. Art. 4(2) stipulates that users and data holders can contractually restrict (or even prohibit *in toto)* such processing that "could undermine security requirements of the connected product, as laid down by Union or national law, resulting in a serious adverse effect on the health, safety or security of natural persons".

Added as a result of the trilogue, the provision seems geared towards upcoming cybersecurity legislation targeting connected products (cf. rec. 115). Art. 4(2) may therefore have been inserted specifically to anticipate the essential cybersecurity requirements for the design of "products with digital elements" pursuant to Art. 13 and Annex I of the Cyber Resilience Act as passed on 12 March 2024 (including regular security updates, amongst other safeguards).[338]

Where the data holder refuses access, this shall be reported to the competent authority in accordance with Art. 37. In light of the comparatively less invasive restriction of access or prohibition of further use, the outright refusal of access must be understood as a last resort given particularly grave health and safety implications. Overall, the reference to "a serious adverse effect on the health, safety or security of natural persons" is indicative of clauses under Art. 4(2) being the strict exception.

Art. 4(3) furnishes the user with instruments of redress (complaints / dispute resolution) in the event they disagree with the data holder on matters connected to the contractual restrictions or prohibitions that have been made pursuant to Art. 4(2).

### Access to Lawfully Processed Personal Data Only (Art. 4(12))

Access to personal data entails their disclosure to the user, typically by way of transmission – and therefore qualifies as processing of personal data according to Art. 4(2) GDPR.[339] To accommodate the ramifications under

338 Commission, Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, COM(2022) 454 final.

339 *In situ*-access by way of a query on the data holder's server infrastructure would also fall within Art. 4(2) GDPR, specifically as data that have been otherwise made available (cf. Roßnagel, A., 'DSGVO Art. 4 Nr. 2 Begriffsbestimmung "Verarbeitung"',

data protection law, a non-dispositive legal barrier to the right to access is set by Art. 4(12). The rule focuses on the scenario where the user is not the data subject whose personal data is being requested. Accordingly, "a valid legal basis under Article 6(1) [GDPR] and, where relevant, the conditions of Article 9 [GDPR] and Article 5(3) [ePrivacy-Directive]"[340] must be shown. As rec. 7 stresses generally, such a legal basis is not found in the fulfilment of the access right itself. *Specht-Riemenschneider* contests this finding based on a contextualisation of Art. 4(12) with Art. 1(5). The former provision would be rendered mostly symbolic if it simply reiterated the continued importance of data protection rules. It is therefore argued that the access right can amount *eo ipso* to a justification of processing, namely to a "legal obligation" as cited by Art. 6(1)(c) GDPR.[341]

*Vice versa*, should the user happen to be the data subject for the personal data being requested, their consent to processing pursuant to Art. 6(1)(a) and 7 GDPR is implicitly given along with the request for access.[342] The same inference of consent can be drawn with respect to Art. 5(3) ePrivacy-Directive, which may also govern access to data sets generated by connected products due to these products being classed as 'terminal equipment'[343] (rec. 36).

Rec. 34 elaborates on the role of users that are not the data subjects at issue. Where they act as enterprises (cf. Art. 2(24), including sole traders) and unless shared household use of the connected product is concerned, these users are considered controllers in the sense of Art. 4(7) GDPR. The burden of demonstrating a valid legal basis for processing would then rest with the user – most likely alongside the data holder, triggering the requirements for joint controllership stated in Art. 26 GDPR.[344] Assuming a kinship with the household exemption under Art. 2(2)(c) GDPR, 'shared

in Simitis, S. / Hornung, G. / Spiecker gen. Döhmann, I. (ed.), Datenschutzrecht: DSGVO mit BDSG, Nomos 2019, para. 26.

340 First suggested by Council Presidency 2022/0047(COD) – 15035/22, pp. 45 et seq.

341 Specht-Riemenschneider, L., *ZEuP* 2023, 638 (665 et seq.).

342 *Ex multis*, Hennemann, M. / Steinrötter, B., *NJW* 2024, 1 (4); Steinrötter, B. *GRUR* 2023, 216 (223); Specht-Riemenschneider, *MMR-Beil.* 2022, 809 (810).

343 See guidance by EDPB, 'Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive' (14 November) para. 16 ("for example, smartphones, laptops, connected cars or connected TVs, smart glasses").

344 Paal, B. / Fenik, M., *ZfDR* 2023, 249 (256).

household use' would for instance not cover company-issued 'smart' wristbands being worn in an employment context.[345]

Especially with respect to Art. 4(12), the Data Act will not ease, let alone resolve the inherent tension between data economy and data protection law by "slicing the Gordian knot"[346] in which both fields of law are entangled. Art. 4(12) presents data holders with dilemmatic choices of immense significance in terms of compliance. They must now find – a nearly impossible mission – the 'correct' boundary between non-personal data and personal data. Failing to provide non-personal data (due to a 'wrong' classification as personal data) could elicit a fine under Art. 40 (and respective national law); providing personal data in breach of data protection law (due to a 'wrong' classification as non-personal data) could likewise result in a fine under Art. 83 GDPR *and* under Art. 40 (if Art. 4(12) is seen as more than a declaratory reference to data protection law[347]). Rec. 34 is of some assistance in this regard by incorporating the rule for so-called mixed data sets as per Art. 2(2) of Regulation (EU) 2018/1807: "Processing of (…) data is subject to the rules established under [the GDPR], including where personal and non-personal data in a data set are inextricably linked."[348]

Even setting aside the quandary of labelling data sets as personal or non-personal, Art. 4(12) requires users that are not a natural person (mostly, enterprises) to evaluate their (subsequent) processing of personal data. Because Art. 6(1)(f) GDPR in particular leaves enormous room for debate[349], users will prefer collecting consent declarations from the data subjects at stake. It is unlikely however that respective users will always be in a *de facto* position to contact data subjects – thus being dependent on the data holder's willingness to intermediate. Data holders, in turn, will also face difficulties in identifying affected data subjects where they diverge from the (enterprise) user – a problem which the Act attempts to remedy

345 Cf. Heinzke, P., *BB* 2023, 201 (205).

346 Hennemann, M. / Steinrötter, B., *NJW* 2022, 1481 (1482); Hennemann, M. / Steinrötter, B., *NJW* 2024, 1 (5).

347 Richter, S., *MMR* 2023, 163 (165); Steinrötter, *GRUR* 2023, 216 (223) (noting the accumulated risk of fines).

348 For information on what is meant by the 'inextricably linked' criterion, see Commission, 'Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union', COM(2019) 250 final, p. 10.

349 See however the suggestion by Specht-Riemenschneider, *ZEuP* 2023, 638 (666) that compliance with the Art. 4(1) access right should influence the weighing of interests under Art. 6(1)(f) GDPR *a priori.*

by recommending "separate accounts for individual [natural] persons" by design (rec. 24).[350]

### Trade Secrets (Art. 4(6)-(9))

*Per se,* the protection of certain data as trade secrets of the data holder does not trump the user's right of access. In no uncertain manner, rec. 31 maintains: "[d]ata holders cannot, in principle, refuse a data access request under this Regulation solely on the basis that certain data is considered to be a trade secret, as this would subvert the intended effects of this Regulation." Sensibly, the Act seeks to balance the competing interests of users and data holders by enabling the disclosure of data to users while "preserv[ing] the protection afforded to trade secrets under [the Trade Secrets Directive]" (rec. 31). Still, it is the user on whose side the chosen legislative approach favouring disclosure errs in Art. 4(6), with the data holder having to show circumstances that legitimise the various defences under Art. 4(7)-(8).[351] Some commentators have gone so far as to describe the user-friendly approach as a system of compulsory licensing to effectuate the access right.[352]

According to the general rule established in the first sentence of Art. 4(6), trade secrets "shall be disclosed only where the data holder and the user take all necessary measures prior to the disclosure to preserve their confidentiality", also and "in particular regarding third parties". By implying that trade secrets shall *only* be disclosed if the necessary measures are taken, Art. 4(6) is formulated in a rather confusing way.[353] The provision should be read with an emphasis on when measures become "necessary". Considering Art. 4(3)(c) of the Trade Secrets Directive, a data holder that is not simultaneously the relevant trade secret holder (cf. Art. 2(19)) has to implement such measures. Should the data holder fail to take necessary

350 Further, cf. Heinzke, P., *BB* 2023, 201 (205).

351 Cf. Macher, E. / Ballestrem, J., *GRUR-Prax* 2023, 661 (661) with details on the legislative history.

352 Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 101 n. 286 et seq.; cf. Heinzke, P., *BB* 2023, 201 (206).

353 Cf. for a discussion of Art. 4(6) in detail Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, pp. 86 et seq.

precautions to preserve confidentiality, the disclosure of the trade secrets represented within the data at issue will be deemed unlawful.[354]

The second sentence of Art. 4(6) specifies that the necessary measures taken by the data holder comprise proportionate technical and organisational measures (TOM)[355], which are exemplified by model contractual terms (cf. Art. 41), confidentiality agreements, strict access protocols, technical standards (cf. Art. 11) and the application of codes of conduct. Most notably, non-disclosure agreements (NDAs) with penalty clauses in the event of a breach of confidentiality are bound to play a pivotal rule.[356] Even though NDAs may form part of the data licensing agreement with the user, this further layer adds to the complexity of the general contractual setting, especially vis-à-vis consumers.[357]

Perhaps most importantly, in its second sentence, Art. 4(6) places the data holder (or a divergent trade secret holder) under the obligation "to identify the data which are protected as trade secrets, including in the relevant metadata". The atypical assessment of trade secrecy *ex ante*, i.e. before the data holder has sued for infringement, presents the data holder with considerable leeway in negotiating the NDA because they can make sweeping claims about data sets containung trade secrets.[358] In line with Art. 9(1) of the Trade Secrets Directive, the onus of trade secrets being affected is namely met if the risk of disclosure is demonstrated to be more likely than not.[359]

To discourage strategic "overclaiming"[360], *Schmidt-Kessel* argues that the data holder – representing the user's interests in a quasi-fiduciary capacity – should separate out data sets involving trade secrets from the outset to the best of their abilities for Art. 4(6)-(8) so as not to obstruct the user's access

354 Cf. Schweitzer, H. / Metzger, A., *ZEuP* 2023, 42 (75).
355 Hennemann, M. / Steinrötter, B., *NJW* 2024, 1 (4).
356 Bomhard, D. / Merkle, M., *RDi* 2022, 168 (171).
357 Hennemann, M. / Steinrötter, B., *NJW* 2022, 1481 (1484); Paal, B. / Fenik, M., *ZfDR* 2023, 249 (258).
358 Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 101 n. 280 et seq.; in agreement: Kerber, W., *GRUR-Int.* 2023, 120 (126); Ducuing, C. / Margoni, T. / Schirru, L. (ed.), *CiTiP Working Paper* 2022, pp. 81 et seq. (noting the more serious consequences in the context of Art. 5(9)).
359 Pauly, D.A. / Wichert, F. / Baumann, J., *MMR* 2024, 211 (212) with further references.
360 Wiebe, A., *GRUR* 2023, 227 (234).

right.[361] Crucially, this could be accomplished at the level of product design so that these data do not become readily available data in the first place.[362]

At any rate, leaving the process of identifying trade secrets in the IoT-generated data to the data holder *ex ante* is consequential. Whereas derived or inferred data (cf. rec. 15) are excluded from consideration, other IoT-generated data sets are capable of trade secret protection within the meaning of Art. 2(1) of the Trade Secrets Directive.[363] In particular, the curation and aggregation (cf. rec. 33) of "raw" sensor data from multiple data points prior to further analysis may reveal not generally known and therefore commercially valuable information about the functionalities and design of a connected product.[364] It seems plausible however that this would not include the mere prospect or probability of aggregation between a plurality of users' data at the hands of a third party.[365] From a practical perspective, close evaluation of the trade secrets regime interacting with the access right pursuant to Art. 49(1)(f) will be needed.

Art. 4(7) addresses the potential failures of disclosing trade secrets pursuant to Art. 4(6). Failures can arise from (1) no agreement on the necessary measures preserving confidentiality having been reached, (2) the user not having implemented the measures or (3) the user undermining the confidentiality of the trade secrets (e.g., by violating Art. 4(11)). Under these circumstances, the data holder is given a right of retention[366]: they can withhold or (apparently in the case of continuous access) suspend sharing "data identified as trade secrets" with the user. The duly substantiated decision must be provided to the user in writing without undue delay while specifying which of the above scenarios (no agreement / failure of implementation / undermining user behaviour) applies.[367] Additionally, the data holder has to notify the competent authority (cf. Art. 37), an obligation

361 Schmidt-Kessel, M., *MMR-Beil.* 2024, 75 (81) ("*Trennungsgebot*").
362 Macher, E. / Ballestrem, J., *GRUR-Prax* 2023, 661 (662).
363 This was prominently denied for raw machine-generated data by the Commission, 'Building a European Data Economy' Commission, COM(2017) 9 final, p. 10.
364 In-depth: Grapentin, S., *RDi* 2023, 173 (174 et seq.); similarly, Wiebe, A., *GRUR* 2023, 227 (232); Heinzke, P., *BB* 2023, 201 (206); Hartmann, B. / McGuire, M. / Schulte-Nölke, H., *RDi* 2023, 49 (54) contend that aggregated data are of no concern in the context of Art. 5(9) due to purpose-specificity, thereby overlooking Art. 4(6).
365 Grapentin, S., *RDi* 2023, 173 (177).
366 Schmidt-Kessel, M., *MMR-Beil.* 2024, 75 (79) ("*Zurückbehaltungsrechte*").
367 Pauly, D.A. / Wichert, F. / Baumann, J., *MMR* 2024, 211 (213).

which could make data holders more reluctant to exercise the right of retention.[368]

Art. 4(8) considers the situation that despite the implementation of measures in line with Art. 4(6), the data holder may exceptionally face a high likelihood of "serious economic damage" due to the disclosure of trade secrets to the user. Here, the data holder is entitled to refuse an access request entirely, but only if they can substantiate that serious economic damage is likely to occur based on "objective elements". Even with the three examples for such objective elements given in the second sentence of Art. 4(8), demonstrating that one user's request has such dire consequences for the data holder will be virtually impossible *in praxi*[369] and should be weighed against the interests of the user in obtaining the data.[370] Again, bringing this defence against the user's request for access is conditional upon notifying the competent authority (cf. Art. 37).

Should the user wish to challenge the defences invoked with reference to the two preceding paragraphs, Art. 4(9) furnishes them with redress mechanisms (complaints / dispute resolution).

### Restrictions on Onward Usage: Non-Compete (Art. 4(10)) and Sharing with Gatekeepers (Art. 5(3)(c))

When compared to the position of data holders (restricted by Art. 4(13)-(14) and the data licensing agreement made thereunder), the user is – at least by default – largely free to use the data as they see fit.[371] Having obtained access, the user must however accept two noteworthy restrictions to this relative freedom of usage.

First, Art. 4(10) stipulates a non-compete obligation of the user.[372] In a regulatory effort to avert outright duplication of the connected product by competitors in the same product (not: geographical) market[373], the user may not use the (personal or non-personal) data made available to them to

368 Hennemann, M. / Steinrötter, B., *NJW* 2024, 1 (4).
369 Grapentin, S., *RDi* 2023, 173 (176 et seq.).
370 Heinzke, P. / Herbers, B. / Kraus, M., *BB* 2024, 649 (653).
371 Schmidt-Kessel, M., *MMR-Beil.* 2024, 75 (81); on (total) buy-out clauses, cf. sub 2 of this section.
372 *Ex multis*, Paal, B. / Fenik, M., *ZfDR* 2023, 249 (258).
373 Bomhard, D., MMR-Beil. 2024, 71 (73) ("*Nachahmungsschutz*"); Heinzke, P. / Herbers, B. / Kraus, M., *BB* 2024, 649 (654).

> "develop a connected product that competes with the connected product from which the data originate, nor share the data with a third party with that intent and shall not use such data to derive insights about the economic situation, assets and production methods of the manufacturer or, where applicable, the data holder."

Rec. 32 reveals a two-fold underpinning: the aim is to "avoid undermining investment incentives" of the data holder into a connected product, which would happen if competitors were free to develop a "product which is considered to be interchangeable or substitutable by users". At the same time, it is the stated intention of the legislator to stimulate the development of entirely novel (complementary) *services* as well as innovation on aftermarkets (cf. the second sentence of rec. 30). The focus on aftermarket promotion also explains why 'related services' were omitted from the non-compete rule under Art. 4(10) in the Act's final version.[374] Moreover it is solely[375] in an aftermarket context that rec. 32 declares permissible reverse engineering the characteristics of a connected product from the data obtained, namely for maintenance and analytics purposes. Overall, the distinction between substitutes and (aftermarket) complements within the non-compete rule has been criticised for lacking a comprehensive economic justification.[376] In particular, the rule is called into question for overlooking the (not infrequent) value creation by data holders through the provision of related services[377] and for effectively hindering users to switch to a competing product manufacturer.[378] Lastly, the consequences of *the user* violating Art. 4(10) remain unclear.[379]

Second, the user is barred from sharing the data they have obtained under Art. 4(1) with a third party designated as a gatekeeper pursuant to Art. 3 DMA. Misplaced in Art. 5(3)(c), this prohibition concerns the user's

374 By contrast, related services had formed part of prior (pre-trilogue) versions of the non-compete rule, but not of the initial Commission proposal; cf. Schweitzer, H. / Metzger, A., *ZEuP* 2023, 42 (61).

375 Unclear on this aspect: Heinzke, P. / Herbers, B. / Kraus, M., *BB* 2024, 649 (654).

376 Cf. Krämer, J., Improving The Economic Effectiveness of the B2B and B2C Data Sharing Obligations in the Proposed Data Act, CERRE, 2022, pp. 23 et seq.; Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, pp. 88 et seq.

377 Heinzke, P. / Herbers, B. / Kraus, M., *BB* 2024, 649 (654).

378 Schweitzer, H. / Metzger, A., *ZEuP* 2023, 42 (61).

379 Hennemann, M. / Steinrötter, B., *NJW* 2022, 1481 (1484); for violations by the data recipient, cf. Art. 6(2)(e), read jointly with Art. 11(2) and (3)(b).

freedom of onwards usage and should hence be merged with a discussion of Art. 4(10).[380]

380 Similarly, Schmidt-Kessel, M., *MMR-Beil.* 2024, 75 (79).