XI. Implementation and Enforcement (Art. 37-42)

Chapter IX ('Implementation and Enforcement', Art. 37-42) lays down the implementation and enforcement framework with regard to competent authorities in each member state, including a complaints mechanism and cooperation with data protection authorities.[887] Thereby, Chapter IX focuses on public enforcement and fails to address private enforcement. However, the mentioning of collective actions in rec. 108 as well as direct references to contractual relationships throughout the Data Act (e.g., Art. 13(1)) imply private enforcement.[888]

1. Competent Authorities (Art. 37)

According to Art. 37(1) and rec. 107, member states should designate one or more competent authorities to ensure the application and enforcement of the Data Act. The member states can either establish new authorities or rely on existing ones. The competent authorities should cooperate with each other, Art. 37(2). If a member state designates more than one competent authority, it should also designate a data coordinator from among them to facilitate cooperation between the competent authorities and to assist the entities in the scope of the Data Act on all matters related to its enforcement and implementation, Art. 37(2).

Therefore, the Data Act opts for a decentralised (member state-driven) enforcement structure which corresponds to the policy of the DGA (but contrasts the policy of the DMA and partially also of the DSA).[889]

The competent authorities shall remain impartial and free from any external influence, whether direct or indirect, and shall neither seek nor take instructions from any other public authority or any private party, Art. 37(8). The member states should ensure that the competent authorities are provided with the necessary resources to this end, Art. 37(9). According

887 Commission COM(2022) 68 final Explanatory Memorandum, p. 16.

888 Furthermore, Art. 10(7) assumes that national courts take cases on FRAND litigation.

889 Krämer, J. et al. Data Act: Towards a balanced EU data regulation, CERRE report, March 2023, p. 32.

to Art. 37(4)(b), the competent authority responsible for the application and enforcement of Art. 23 to 31 and Art. 34 and 35 shall have experience in the field of data and electronic communications services.

Where either the protection of personal data or specific sectoral data access and use issues are concerned the respective competent authorities should also have the responsibility for the application of the Data Act in the respective fields, Art. 37(3) and Art. 37 (4)(a). When a member state designates more than one competent authority which monitor sectors in an overlapping manner, their competences have to be distributed carefully between them.[890]

Member states should clearly define the tasks and powers of the competent authorities which – according to Art. 37(5) – should include among others promoting data literacy and awareness of the rights and obligations under the Data Act (a) and monitoring technological and commercial developments of relevance for the making available and use of data (e). According to Art. 37(5)(b) they should especially handle complaints arising from alleged infringements of the Data Act. They should also investigate the subject matter of complaints as well as matters that concern the application of the Data Act, including on the basis of information received from another competent authority or other public authority (c). The legislator further elaborates on these powers of investigation and especially the cooperation of the competent authorities regarding investigations in rec. 107.

According to Art. 37(5)(d) the competent authorities should impose effective, proportionate and dissuasive financial penalties which may include periodic penalties or penalties with retroactive effect as well as initiating legal proceedings for the imposition of fines.[891] While Art. 40 is not solely focused on financial penalties, only this type of penalty is mentioned in Art. 37(5).[892] Competent authorities should cooperate with competent authorities of other member states and, where relevant, with the Commission or the EDIB (f); with the relevant competent authorities responsible for the implementation of other Union or national legal acts (g) and with the relevant competent authorities to ensure that Art. 23 to 31 and Art. 34 and 35 are enforced consistently with other Union law and self-regulation applicable to providers of data processing services (h). This cooperation

890 Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 117.

891 Cf. also below sub XI. 4.

892 Wiebe, A., *GRUR* 2023, 227 (237).

should be facilitated by the data coordinator if one is designated (Art. 37(5) subpara. 2).

According to Art. 37(6), the data coordinator if designated should:

"(a) act as the single point of contact for all issues related to the application of this Regulation;
(b) ensure the online public availability of requests to make data available made by public sector bodies in the case of exceptional need under Chapter V and promote voluntary data sharing agreements between public sector bodies and data holders;
(c) inform the Commission, on an annual basis, of the refusals notified under Article 4(2) and (8) and Article 5(11)".

The Commission should maintain a public register of the competent authorities based on the information the member states should communicate, Art. 37(7).

According to Art. 37(14) competent authorities have the power to request all the information that is necessary to verify compliance with the requirements of the Data Act from users, data holders and data recipients or their legal representatives. These requests have to be proportionate to the performance of the task and should be reasoned. Competent authorities can also submit a reasoned request for assistance or enforcement from a competent authority in another member state. Upon receiving such a request, the respective other authority should provide a response without undue delay, detailing the actions that have been taken or which are intended to be taken (Art. 37(15)).

Competent authorities should respect the principles of confidentiality and of professional and commercial secrecy and should protect personal data in accordance with Union and national law, Art. 37(16). Any information exchanged in the context of assistance requested and provided under Art. 31 should only be used in respect of the matter for which it was requested (Art. 37(16)).

Jurisdiction concerning Entities within the Scope of the Data Act

Art. 37(10) also regulates the jurisdiction of which member state an entity will be subject to. This is the member state in which it is established or in which it has its main establishment. As its main establishment will be considered where it has its head office or its registered office within which

the principal financial functions and operational control of the entity are exercised.

Entities within the scope of the Data Act should also designate a legal representative in one of the member states (Art. 37(11)). The entity should mandate the legal representative to be addressed in addition to or instead of the entity itself regarding all issues related to the compliance with the Data Act (Art. 37(12)). The legal representative should cooperate with the competent authorities and comprehensively demonstrate to them upon request, the actions taken, and provisions put in place by the entity to ensure compliance (Art. 37(12)).

An entity is deemed to be under the jurisdiction of the member state in which the legal representative is located, Art. 37(13) sent. 1. The designation of a legal representative should be without prejudice to any legal actions which could be initiated against the entity, Art. 37(13) sent. 2. Until an entity has designated a legal representative it will be under the competence of all member states, so that any competent authority may exercise its competence if the same entity is not subject to enforcement proceedings under the Data Act for the same facts by another competent authority (Art. 37(13)).

2. Right to Lodge a Complaint with a Competent Authority (Art. 38)

In order to enforce their Data Act rights, natural and legal persons should be entitled to seek redress for the infringements of their rights under the regulation by lodging complaints with competent authorities (Art. 38(1) and rec. 108). These complaints can be lodged individually or collectively. The data coordinator should upon request provide all the necessary information to natural and legal persons for lodging their company to the appropriate competent authority, Art. 38(1) sent. 2.

According to Art. 38(2) the competent authority with which the complaint has been lodged shall inform the complainant of the progress of the proceedings and of the decision taken in accordance with national law (similarly to Art. 58(4) GDPR).[893]

Competent authorities should be obliged to cooperate to ensure the complaint is appropriately handled and resolved effectively and in a timely manner (Art. 38(3) and rec. 108). The cooperation should include exchanging all relevant information by electronic means without undue delay,

893 Remke, C., *MMR-Beil.* 2024, 117 (119).

however without any effect on the cooperation mechanisms provided for by Chapters VI and VII of Regulation (EU) 2016/679 and by Regulation (EU) 2017/2394, Art. 38(3).

The right to lodge a complaint under Art. 38 is without prejudice to any other administrative or judicial remedy (Art. 38(1)), thus not precluding private enforcement.[894] Despite the focus on contractual relations in the Data Act, it does not address comprehensively the role of private enforcement.[895] This lack of harmonisation of private enforcement may lead to disharmony concerning claims by users, but also unfair competition law-based actions and national legislation on private remedies concerning the rights under the Data Act.[896] Harmonisation could have also clarified the relationship between public enforcement and private remedies.[897]

3. Right to an Effective Judicial Remedy (Art. 39)

Art. 39(1), (2) regulates the right to an effective judicial remedy with regard to legally binding decisions taken (or failures to act) by competent authorities. Any affected natural and legal person has a respective right notwithstanding any administrative or other non-judicial remedies. The proceedings pursuant to Art. 39 should be brought before the courts or tribunals of the member state of the competent authority against which the judicial remedy is sought, Art. 39(3).

4. Penalties (Art. 40)

The member states should lay down rules on penalties applicable to infringements of the Data Act. Penalties shall be effective, proportionate and

894 Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 118; Steinrötter, B., *GRUR* 2023, 216 (225).

895 Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 118; Schwamberger, S., Der Datenzugang im Data Act: Fortschritt oder Rückschritt?, in: Bernzen, A. K. et al., Immaterialgüter und Medien im Binnenmarkt, Nomos 2022, p. 88 (110); Steinrötter, B., *GRUR* 2023, 216 (225).

896 Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 118.

897 Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 119.

dissuasive, and should take all measures necessary to ensure that they are implemented (Art. 40(1)). Rec. 109 gives as examples "financial penalties, warnings, reprimands or orders to bring business practices into compliance with the obligations imposed by" the Data Act.

Until the Data Act applies, the member states should notify the Commission of those rules and measures as well as of any subsequent amendment affecting them (Art. 40(2)). The Commission should maintain and regularly update an easily accessible public register of those measures.

Additionally, rec. 109 states that it is the task of the competent authorities to ensure that infringements of the obligations laid down in the Data Act are sanctioned by penalties. Art. 40(3) and rec. 109 add a list of non-exhaustive and indicative criteria for the imposition of penalties, such as for example the nature, gravity, scale and duration of the infringement (a) in view of the public interest at stake, the scope and kind of activities carried out, and the economic capacity of the infringing party; whether the infringing party systematically or recurrently fails to comply with its obligations under the Data Act and any action taken by the infringing party to mitigate or remedy the damage caused by the infringement (b).

As Art. 40 leaves it to the member states to lay down rules, different standards within the member states are possible.[898] Additionally, the data protection authorities remain competent to impose administrative fines for the infringement of the GDPR.[899] Altogether this may lead to overlapping and parallel enforcement and thus to inefficient results and legal uncertainty.[900] This is partly addressed by Art. 40(3), stating that the member states should take into account the recommendations of the EDIB.

Rec. 109 adds that – in order to avoid that the same infringement is penalised more than once – a member state that intends to exercise its competence in relation to an infringing party that is not established and has not designated a legal representative in the Union should – without undue delay – inform all data coordinators as well as the Commission.

898 Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 118.

899 Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 118.

900 Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 118.

Concerning the role of the EDIB[901] for imposing penalties, rec. 110 adds:

> "Among other functions, the competent authorities should make use of the EDIB as a platform to evaluate, coordinate and adopt recommendations on the setting of penalties for infringements of this Regulation. It should allow for competent authorities, with the assistance of the Commission, to coordinate the optimal approach to determining and imposing such penalties. That approach prevents fragmentation while allowing for Member State's flexibility, and should lead to effective recommendations that support the consistent application of this Regulation."

5. Model Contractual Terms (Art. 41)

In order to assist parties in drafting and negotiating contracts with fair, reasonable and non-discriminatory contractual rights and obligations, the Commission should develop and recommend non-binding model contractual terms on data access and use as well as non-binding standard contractual clauses for cloud computing contracts, Art. 41. The first should include "reasonable compensation and the protection of trade secrets".

According to rec. 111 model contract terms should also "where necessary take into account the conditions in specific sectors and the existing practices with voluntary data sharing mechanisms". This should be done before the 12.09.2025.[902] Rec. 111 further explains:

> "These model contractual terms should be primarily a practical tool to help in particular smaller enterprises to conclude a contract. When used widely and integrally, these model contractual terms should also have the beneficial effect of influencing the design of contracts about access to and use of data and therefore lead more broadly towards fairer contractual relations when accessing and sharing data."

The model contractual terms and the standard contractual clauses are an important instrument for making the Data Act work effectively in prac-

901 On the role of the EDIB in general cf. below XI. 6.

902 The Commission has set up an expert group to help draft the model contractual terms which plans to recommend them by autumn 2025: https://digital-strategy.ec.europa.eu/en/policies/data-act-explained.

tice.[903] Thus, *Leistner* and *Antoine* point to draft model contract terms for data sharing on a contractual basis, on the necessary protection of trade secrets, the fairness test for B2B data sharing contracts and the minimum content for cloud service contracts defined in Art. 24.[904]

With a similar aim of assisting parties in drafting and negotiating contracts with balanced contractual rights and obligations, the American Law Institute (ALI) and the European Law Institute (ELI) developed "Principles for a Data Economy", which do function as an example and / or blueprint for the model contractual terms and standard contractual clauses.[905] The same holds true for the default rules on data provision contracts currently developed by the UNCITRAL Working Group IV.[906]

6. Role of the European Data Innovation Board (Art. 42)

The EDIB that has been set up[907] under Art. 29 DGA[908] as a Commission expert group should also support the consistent application of the Data Act. It should thus advise and assist the Commission developing a consistent practice of competent authorities (Art. 42(a)). It should also facilitate cooperation between competent authorities through capacity-building and the exchange of information as well as comprehensive discussions between the competent authorities (Art. 42(b) and rec. 110). This shall "increase

903 Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 119.

904 Leistner, M. / Antoine, L., IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 119.

905 See https://europeanlawinstitute.eu/projects-publications/completed-projects/data-economy/.

906 UNCITRAL, Report of the Working Group IV (Electronic Commerce) on the work of its sixty-fifth session (New York, 10–14 April 2023), A/CN.9/1132, pp. 3 et seq.; UNCITRAL, Working Group IV (Electronic Commerce), Sixty-fifth session, New York, 10–14 April 2023, Default rules for data provision contracts, A/CN.9/WG.IV/WP.180; UNCITRAL, Report of the Working Group IV (Electronic Commerce) on the work of its sixty-sixth session (Vienna, 16–20 October 2023), A/CN.9/1162, pp. 10 et seq.; UNCITRAL, Working Group IV (Electronic Commerce) Sixty-sixth session, Vienna, 16–20 October 2023, Default rules for data provision contracts (first revision), A/CN.9/WG.IV/WP.183.

907 Further details: https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?lang=en&groupID=3903.

908 Commentary on Art. 29 DGA: Hennemann, M., in: Specht-Riemenschneider, L. / Hennemann, M., Data Governance Act, 2023, Art. 29 DGA.

effective access to justice as well as enforcement and judicial cooperation across the Union", rec. 101.

Especially, it shall advise and assist with regard to the request of the drafting of harmonised standards (Art. 33(4), Art. 35(4) and Art. 36(5)), the preparation of the drafts of the implementing acts (Art. 33(5), Art. 35(5), (8) and Art. 36(6)), the preparation of the delegated acts (Art.29(7) and Art. 33(2)) and the adoption of guidelines laying down interoperability specifications for the functioning of common European data spaces (Art. 33(11)).

Rec. 110 further explains, that the EDIB should "advise and assist the Commission in coordinating national practices and policies on the topics covered by the Data Act as well as in delivering on its objectives in relation to technical standardisation to enhance interoperability."