3 March 2022

The Data Act – Sharing is Caring. Or Is It?

On 23 February 2022 the European Commission (Commission) published its draft proposal for a regulation on harmonized rules on fair access to and use of data (Data Act) (COM(2022) 68 final). The Data Act, which builds on the Data Governance Act (COM(2020) 767 final), aims to facilitate the access to and exchange of data between, in particular, businesses as a major resource in the age of digitalization and the so-called industry 4.0. The relevance of data as a resource has been at the forefront of the legislative agenda both nationally and on the EU-level in the last years. Apart from the General Data Protection Regulation (GDPR), which concerns the protection of personal data, initiatives like the EU's Digital Markets Act (DMA) or the 10th amendment of the German Act Against Restraints of Competition (ARC) address, inter alia, the importance of data and the potential competitive harm of foreclosing access to data. However, the Data Act is by far the most ambitious project as it has the potential to remodel the way data is handled in the EU and beyond. This blogpost takes a first look at the Commission's proposal and, in particular, the (potential) nexus to antitrust law.

I. INTRODUCTION

The Data Act is part of the Commission's data agenda laid out in its communication "A European Strategy for Data", which was published on 19 February 2020 (COM(2020) 66 final). It must be seen in the wider context of the Commission's broader policy goals set out in "A Europe Fit for the Digital Age".

In its data strategy, the Commission describes its vision for a "*data-agile*" European economy and has identified data access and sharing between, *inter alia*, businesses as a prerequisite and the accumulation of data in the hands of a few players as a major threat for its vision of "*a genuine single market for data*" (Commission, A European Strategy for Data, p 3, 4, 6 et seq). The Commission's data strategy was welcomed by the European Parliament in its resolution on a European strategy for data (2020/2217(INI)) of 25 March 2021.

Against this background, the Data Act is designed to lay the ground for data sharing and is supposed to act as major contributor to the data-agile economy. In the words of the Data Act: "*The aim [is] to ensure fairness in the allocation of data value among actors in the data economy and to foster access to and use of data*" (p 2 of the Commission's proposal).

The Data Act complements the Data Governance Act, which is set to enter into force in the first half of 2022 and which, most notably, addresses the re-use of public sector data and sets up a regulatory framework for data intermediaries. In addition, the Data Act has several important intersections to existing and future "vertical" data regulation such as the Payment Service Directive (2015/2366) for the financial sector and, in particular, the DMA as well as competition law in general (p 3 et seq of the Commission's proposal).

II. OVERVIEW

The legal basis for the Data Act is Art 114 of the Treaty on the Functioning of the European Union (TFEU), which allows the Commission to implement rules that advance the internal market.

Pursuant to Art 1(1), the Data Act creates a framework for the basic access to and exchange of data, with data being defined broadly as "*any digital representation of acts, facts, or information and any compilation of such acts, facts or information, including in the form of sound, visual or audio-visual recording*" (Art 2(1) Data Act).

The Data Act is business sector agnostic. It is a "horizontal" regulation and applies to virtually all businesses no matter their products or services. Accordingly, apart from some exceptions for micro or small enterprises pursuant to Art 2 of the Annex to Recommendation 2003/361/EC (Art 7 Data Act), data holders and data recipients must comply with the Data Act. This alone shows the significant impact the Data Act would have. It would apply to any producer or provider of Internet-of-Things (IoT) products or related services, be it vehicles that drive autonomously, voice assistants, cellphones, smart machinery of any type, smart home appliances, medical and health devices, etc. (Art 1(2)(a), Recital 14 Data Act).

The Data Act's 42 Articles are divided up into 11 chapters, which cover the following topics:

- Chapters II and III contain the main rules concerning **business to business (B2B) and business to consumer (B2C) data sharing** with a particular focus on access to data generated by use of IoT products or related services.

- Chapter IV defines **unfair contractual terms** that shall not be used *vis-à-vis* micro, small or medium-sized enterprises with respect to data access and use of data.

- Chapter V regulates **business to government (B2G) data sharing** where there is an exceptional need for data by public authorities.

- Chapters VI, VII and VIII address the **switching between and interoperability of data processing services** like cloud providers (including rules on smart contracts) and the access and transfer of (non-personal) data internationally.

- Chapter IX includes rules on **public enforcement**, which will – unlike for the DMA – rest with the member states, which "*shall designate one or more competent authorities as responsible for the application and enforcement of this Regulation*" (Art 31 Data Act).

- Chapters X and XI contain miscellaneous provisions, which, *inter alia*, stipulate that the rules of the Data Act shall **apply 12 months after its entry into force**.

The remaining part of this blogpost will focus on the data access rules contained in chapters II and III and their enforcement as they have the potential to be a gamechanger in the handling of non-personal data and thus would have a profound impact on businesses.

III. IOT DATA SHARING, CHAPTER II

Chapter II is the heart of the Data Act because it contains extensive data sharing obligations with a view to IoT products or related services between, *inter alia*, businesses.

Access by design

Art 3(1) Data Act stipulates that data generated using IoT products or related services shall be accessible by design: "*Products shall be designed and manufactured, and related services shall be provided, in such a manner that data generated by their use are, by default, easily, securely and, where relevant and appropriate, directly accessible to the user*". In addition, pursuant to Art 3(2) Data Act, users of such products or services shall be provided with the relevant information to understand the availability of the generated data.

The notion of accessibility by design is potentially far reaching, as (i) any producer of IoT products, namely, any product that "*obtains, generates or collects data concerning its use or environment*" (Art 2(2) Data Act), or (ii) related services, namely, any "*digital service, including software, which is incorporated in or inter-connected with a product in such a way that its absence would prevent the product from performing one of its functions*" must comply and ensure that easy and secure data access is possibly for the user by default. However, as of yet, the Data Act does not provide further guidance as to the conditions for a product or service to be deemed in compliance with Art 3(1) Data Act.

Despite the difficulties in determining the standard of accessibility, the obligation under Art 3(1) Data Act has the potential to transcend the Data Act. If IoT products, be it consumer or industry IoT, were accessible by design, this would also have a significant impact on data access and sharing obligations beyond the Data Act as it could reduce the practical hurdles faced, for instance, with respect to an industry 4.0 data sharing obligation under already existing Sec 20 para 1a ARC.

Access to data

Art 4 Data Act stipulates that any user of any IoT product or related service (consumer or business) has a right to access and use data generated using the IoT products or related services *vis-à-vis* the data holder, namely, any "*legal or natural person, who has the right or obligation […] or […] through control of the technical design of the product or related service, the ability to make available certain data*" (Art 2 no 6 Data Act).

Going even further, Art 5(1) Data Act stipulates that "*upon request by a user, or by a party acting on behalf of a user, the data holder shall make available the data generated by the use of a product or related service to a third party*." The data made available to the third party must have the same quality as is available to the data holder and, where applicable, must also be provided continuously and in real-time. In this context, it is worth noting that Art. 5(2) Data Act excludes undertakings that provide platform services which have been designated as gatekeeper under the DMA, as an eligible third party within the meaning of Article 5(1) Data Act. Accordingly, a data user could not share machine data with such undertaking under the Data Act.

The practical implications Art 4 and 5 may have on the so-called industry 4.0 are immense. Art 5 Data Act basically means that any (business) user of any IoT product, e.g., smart machinery of any kind, and (almost) any third party having the consent of said user must be given access to data that is generated by the IoT product or related service. The Commission itself flags the (obvious) relevance of the third-party data access for aftermarket situations, namely, the repair of IoT products or services like predictive maintenance (Recitals 6, 28 and Q&A Data Act).

However, the Data Act would not introduce a general right to third-party data access. Any third-party rights under Art 5 Data Act are derived from the individual IoT user. A third party would thus not be able to request non-individual data access from any producer of IoT products or provider of related services. Furthermore, the right to access under the Data Act is confined to the data itself. Non-individual data access, access to software or interoperability on a wider scale could only be requested under antitrust law or via other types of access regulation such as the DMA, provided the respective requirements are met.

In stark contrast to the broad access rights of the user and third parties, Art 4(6) and Art 5(5) Data Act would limit the data holder's own right to use generated data. Unless contractually agreed upon, the data holder would not be allowed to use non-personal data generated by using the product or related service. A highly questionable approach given the producers' need to access data to continuously improve and monitor the safety of IoT products such as autonomous vehicles or smart machinery.

IV. GENERAL OBLIGATIONS FOR DATA HOLDERS, CHAPTER III

Chapter III sets out general provisions in relation to any obligation to make data available. Such obligation may originate from the Data Act itself, namely, Art 5, or any "*other Union law or national legislation implementing Union law*" that comes into force after the date of application of the Data Act (Art 12(3), Art 41(2) Data Act). Against this background, the (future) reach of Chapter III may be significant.

Pursuant to Art 8(1) Data Act, a data holder who is obliged to make data available to a third party under Art 5 Data Act must apply fair, reasonable and non-discriminatory (FRAND) terms and act transparently. In addition, Art 9(1) Data Act stipulates that any compensation for access and use of data shall be reasonable, and that the data holder must provide the necessary

information on the calculation so that the data recipient may assess whether the compensation is in fact reasonable (Art 9(4) Data Act).

Art 8 and 9 Data Act build heavily on the FRAND criteria that feature prominently in the Art 102 TFEU obligations on holders of standard essential patents (SEP). Accordingly, provided the relevant provisions enter into force, there is much to be learned from antitrust law with a view to the procedural obligations as defined by the ECJ in *Huawei/ZTE* and further spelled out by national courts. Despite the reasonableness of referring to the FRAND criteria regarding data access in general, SEP litigation shows that perceptions of what is in fact FRAND may differ significantly.

Finally, the data access rules enshrined in Art 8 and 9 Data Act could go beyond their direct scope of application. With a view to the relevance of data access in competition law and the DMA, they may very well develop into a blueprint of how data access can be handled in a more general way.

V. ENFORCEMENT, CHAPTER IX

Public Enforcement

Pursuant to Art 31 Data Act, the Member States are responsible for the public enforcement: "*Each Member State shall designate one or more competent authorities as responsible for the application and enforcement of the Data Act*". The designated authorities must be equipped to levy penalties that are "*effective, proportionate and dissuasive*" (Art 33(1) Data Act). Beyond this general obligation, Art 33(3) Data Act defines that a violation of any obligation laid down in chapters II, III and V of the Data Act is punishable with fines in maximum amounts of EUR 20 million or 4 percent of global turnover, whichever is higher.

Private Enforcement

The Data Act does not contain a dedicated private enforcement regime. However, Art 10 Data Act envisages a dispute settlement regime that allows data holders and data recipients to settle any conflicts about data sharing or access, although decisions shall only be binding if agreed upon by the parties to the proceeding (Art 10(8) Data Act).

Beyond that, Art 10(9) Data Act explicitly states that *"[t]he Article does not affect the right […] to seek an effective remedy before a court or tribunal of a Member State*". Private enforcement before national courts would thus be an option if the Data Act were to enter into force. Given the sheer quantitative relevance of the data sharing obligations laid down in chapters II and III of the Data Act, private enforcement would probably be of relevance especially in aftermarket situations.

VI. OUTLOOK

The Data Act is an important building block of the Commission's regulatory scheme for the digital economy.

While it remains to be seen how the certainly ambitious Data Act fairs in the upcoming legislative process and how much watering down will take place, the Commission appears serious about its vision of "*a genuine single market for data*". The Data Act has the potential to fundamentally reshape the regulatory landscape for data handling in the EU. Accordingly, companies should take a close look at the Commission's draft to assess how their business model might be – positively or negatively – affected and follow the developments closely to be prepared.

Contact

DR MAX SCHULZ

Associate

Phone: +49 211 20052-360
Email: m.schulz@glademichelwirtz.com

DR SIMON WEISE

Associate

Phone: +49 211 20052-420
Email: s.weise@glademichelwirtz.com