

# Kluwer Competition Law Blog

## The Data Act: A Stepping Stone for a New Data Economy?

Teodora Groza (Sciences Po Law School) · Friday, December 15th, 2023

Overshadowed by the outsize attention surrounding the AI Act Trilogue, the EU passed in late November another regulatory instrument with transformative potential for the digital economy: [the Regulation on harmonised rules on fair access to and use of data \(Data Act\)](#). Admittedly, the Data Act is not as groundbreaking as the AI Act. Far from being the first of its kind, it will be imbricated in a complex web of overlapping regimes of data governance, stemming from the GDPR to the [Trade Secrets Directive](#) to the recent [Data Governance Act](#). Yet, its transformative potential—or, at least, ambitions—should not be underestimated. In the following, I explain 1) the scope of the act and its main ambitions, and 2) what has changed since the draft version of the Act, while highlighting the impact of these changes on market competition and market structures.

### The Data Act at a glance: fairness through markets

The granularities of the Data Act were skillfully covered on this platform in a [post](#) published shortly after the release of the draft version of the regulation. Since the bulk of the Act has remained unchanged, from its structure to its complex relationship with the patchwork of pre-existing regulations, I will not rehearse that discussion. Rather, I will briefly restate the scope of the Act and its main normative ambitions, as well as the key legal moves reflecting these ambitions. Whereas the Act covers not only business-to-business (B2B) data sharing but also business-to-government (B2G) and switching between data processing services, in the following, I focus on B2B data sharing due to its consequential impact on market competition.

The Data Act applies to a narrow category of data: data generated by the use of connected devices—or, in day-to-day language, Internet of Things (IoT) devices. These devices have gradually infiltrated our daily existence. For some of us, they perform minor functions, like robot vacuum cleaners or connected fridges. Yet for others, they are at the heart of their economic livelihoods—think of users making a living off farming, for whom smart tractors are vital infrastructure. As more and more devices become “connected,” the Data Act will mature into a key regulatory instrument. Any attempts at dwarfing its relevance or dismissing it due to its narrow scope are premature.

The Data Act’s overarching objective is to ensure fairness in the allocation of value generated by data among all actors in the digital environment, from SMEs to end users. Nonetheless, aligned with the EU’s decades-long commitment to creating and fostering markets, the vision of fairness that emerges from the Act is a distinctly marketized one. This is visible in two legal moves. First,

the Act puts forward an alternative approach to data as a resource that is co-generated by the interaction between the user and the connected product. Before the intervention of the Act, the data generated by the use of IoT devices was captured by the product manufacturers who had exclusive, property-like control over it. Contrastingly, the Act seeks to empower users by giving them a say—and a stake—in what can be done with the data generated by their use of IoT devices. To do so, it grants them the right to request that the data they co-produce be shared with third parties active in the aftermarkets of repair and maintenance of the products at stake. The expectation is that sharing this data will benefit users by making after-sale services cheaper and more efficient, as well as by leading to the emergence of innovative services. As my co-author and I have argued [elsewhere](#), this mechanism might fall short of achieving its objectives, since in the absence of immediate and direct benefits users will have little incentive to request their data to be shared. But despite the suboptimal design, the introduction of a mechanism enabling users to use the data they co-produce to their own benefit is a novel and much-welcome development.

Second, the Act is manifestly dedicated to strengthening the position of SMEs in the data economy. To begin with, these enterprises are relieved from the regulatory burden of complying with the data-sharing obligation. The flip side of this exemption is that enterprises designated as gatekeepers cannot benefit from the right of users to ask for their data to be shared. Ultimately, SMEs win twice: first, they don't need to bear the costs of setting up data-sharing mechanisms, and second, they get access to data that the biggest players cannot benefit from. Moreover, the Act prohibits unfair contractual terms related to data access and data use, strengthening the bargaining power of the smallest players. Most notably, data holders sharing data pursuant to a user request cannot limit the use of data to the extent that its value cannot be exploited in an adequate manner, thus preserving the economic relevance of the data being shared. Lastly, the compensation required by data holders cannot include a margin when the data recipient is an SME.

Going back to the market logic of the Act, these legal moves are not justified only by an appeal to fairness, but rather by reference to the concrete economic benefits they are intended to bring about. The underlying narrative is that data sharing will generate huge economic potential by opening up new market opportunities, stimulating a competitive data market, and creating opportunities for data-driven innovation for SMEs that previously lacked data access.

### **From the draft to the final text**

It took more than a year and a half before the draft version of the Data Act matured into its final form. The final version of the Act contains significant changes related to i) clarifying the types of data its various chapters apply to; ii) the relationship between the Act, the GDPR, and data sharing arrangements based on private law agreements between private parties; iii) the types of compensation that can be requested by data holders subject to data sharing obligations; and iv) the protection of trade secrets.

#### *The new data taxonomy*

The final text introduces a new distinction between “*product data*” and “*related service data*”. Product data refers to “*data generated by the use of a connected product that the manufacturer designed to be retrievable from the connected product by a user, data holder or a third party,*

*including [...] the manufacturer*". Related service data covers "*data which also represent the digitisation of user actions or events related to the connected product which are generated during the provision of a related service by the provider*".

Since both types of data cover digitisations of user actions, it is unclear what is the added value of introducing this taxonomy. Moreover, the provisions related to data sharing cover both types of data, further putting into question the necessity of the distinction. In addition to this taxonomy, the final text provides a laundry list of the types of data that are relevant to each of its chapters introduced in Article 1(2). Interestingly, this Article introduces one more category of data—"*private sector data*"—whose scope is not defined anywhere in the Act.

### *The GDPR and private ordering*

The draft version of the Act specified that certain data generated by the use of connected devices will qualify as personal data under the GDPR. This is intuitive: information such as the size of an apartment which can be collected by a connected vacuum cleaner offers indications of the economic status of the natural person using the device. The relationship between the Data Act and the GDPR is complicated by the fact the Act operates with the notions of the "*user*" and the "*data holder*" which do not overlap with the vocabulary of the GDPR and its consecrated notions of "*data subject*" and "*data controller*". Furthermore, the Data Act does not distinguish between owners of connected devices and their users—the Act grants rights and obligations only to users, misleadingly defined as "*natural or legal persons that own a connected product or to whom temporary rights to use that connected product have been contractually transferred*".

To illuminate this tension, take the following examples. When a connected vacuum cleaner is owned and used by the same natural person, the GDPR does not induce any friction in the data-sharing process. But in situations where the owner of the device is an enterprise, and the device is used by—and collects data on—several natural persons, then the device owner will qualify as a data controller within the meaning of the GDPR and will have to provide a legal basis for data processing and requesting that data be shared with third parties. The final version of the Act clarifies that the Act itself does not constitute a legal basis within the meaning of the GDPR. Nonetheless, it indicates that there are several potential avenues to share the data while ensuring compliance with the GDPR: either to obtain consent from the data subject or to anonymize the personal data at stake.

In addition to the GDPR, there is another parallel data governance regime that sits in tension with the Data Act: voluntary data-sharing agreements concluded through private contracting. On the one hand, the final text specifies that voluntary data-sharing agreements between gatekeepers and data holders are unaffected by the Act. This means that the Act does not prevent data from being shared with outside market players—it simply does not recognize an obligation to share data with them. On the other hand, the Act also mentions that voluntary data-sharing agreements are not caught by its requirements that data access should be based on fair, reasonable, non-discriminatory, and transparent terms and conditions. Nonetheless, these carve-outs may easily fall short of insulating data-sharing agreements based on private ordering from the reach of the Data Act. As law and economics scholarship shows, even arms-length bargaining occurs [in the shadow of existing regulations](#), which inform and often influence the content of the agreements the parties reach.

### *Compensation*

Despite being rooted in a philosophy that data sharing represents a key tool for bolstering economic growth, the Data Act is mindful of the trade-off between sharing assets with competitive significance and preserving investment incentives. To reconcile the two objectives, the Act allows data holders to request compensation for data sharing.

If the draft version left the granularities of what compensation can be requested unspecified, the final version of the Act clarifies the limits of reasonable compensation. First, it is meant to cover the costs incurred in making the data available and to reflect the investment in the technical tools necessary to collect, store, and share the data. Importantly, in the case of long-term or recurring data-sharing requests, the Act envisages the use of subscription models of smart contracts to minimize the costs of repeated one-off interactions. Second, reasonable compensation can include a margin—but as highlighted above, such margin is prohibited when the data recipient is an SME or a not-for-profit research organisation.

### *Trade secrets*

Lastly, but perhaps most importantly, the final text provides for enhanced protection of trade secrets. The draft version provided that trade secrets shall be disclosed only when it is strictly necessary to do so and provided that measures to preserve their confidentiality have been taken. Nonetheless, it did not offer data holders the right to refuse to share data on the grounds that trade secrets are concerned.

The final version of the Act grants data holders the right to withhold or suspend sharing data identified as trade secrets, on the condition that it notifies the competent authority and substantiates this decision. Additionally, data holders may refuse data sharing requests altogether on a case-by-case basis when trade secrets are concerned, provided that it can demonstrate that it is likely to suffer serious economic damage from the disclosure of trade secrets.

The heightened protection granted to trade secrets fits within the Act's overall cautiousness towards information sharing between (potential) competitors. The poster child of this approach is the Act's prohibition that the data shared be used for developing a product that competes with the product from which it originates. Whereas this prohibition is motivated by the need to preserve investment incentives, it might have the unintended effect of strengthening the competitive position of manufacturers by insulating them from potential market entry from providers of aftermarket services.

### **A site for regulatory experimentation**

It will be a while before the provisions of the Data Act become applicable—20 months after the date of its entry into force—and even longer before its effects will be perceivable. Nonetheless, a series of observations regarding its future effects can already be expressed.

Despite the already routine disclaimer inserted in most legislative acts that the competition regime remains unaffected, the Act will have consequential impacts on market competition. These effects are not unidirectional. On the one hand, the recognition that data is a key competitive asset that is co-produced by consumers and that they are thereby entitled to a stake in the value it generates is a very welcome development. It also represents a radical departure from the competition law essential facilities doctrine, under which competitors can request forced access to external assets only under strict circumstances. In an ideal scenario in which users will avail of the right to request their data to be shared, the Act might have consequential impacts on business models which aimed at trapping customers into a closed ecosystem of aftermarket services. A notable example of such a business model was [John Deere's policy of locking farmers out of the software of their smart devices](#) in order to prevent repair and maintenance services. In a post-Data Act world, farmers will get to benefit from cheaper and more efficient aftermarket services.

On the other hand, the limitations on leveraging data for the development of competing products, and the right of data holders to refuse to share trade secrets on a case-by-case basis represent significant limitations to the data-sharing regime created by the Act. These are not surprising, though. The EU's overarching approach to information sharing and cooperation between competitors, as reflected for instance in the [R&D block exemption regulation](#), is overly cautious. The path towards opening up the competition framework to more information sharing and collaboration is long.

On an aspirational level, the Data Act might be just the beginning of a new data economy, providing a template for data-sharing agreements across all sectors and showcasing the benefits of data sharing in terms of bolstering market opportunities and stimulating innovation. It might lead to a reconfiguration of the market position of consumers as co-producers of data and of SMEs as stakeholders entitled to data as a key competitive asset. But even if it falls short of these achievements, the Act represents a site of regulatory experimentation, and its transformative potential should not be underestimated.

---

*To make sure you do not miss out on regular updates from the Kluwer Competition Law Blog, please subscribe [here](#).*

## **Kluwer Competition Law**

The **2022 Future Ready Lawyer survey** showed that 79% of lawyers are coping with increased volume & complexity of information. Kluwer Competition Law enables you to make more informed decisions, more quickly from every preferred location. Are you, as a competition lawyer, ready for the future?

Learn how **Kluwer Competition Law** can support you.

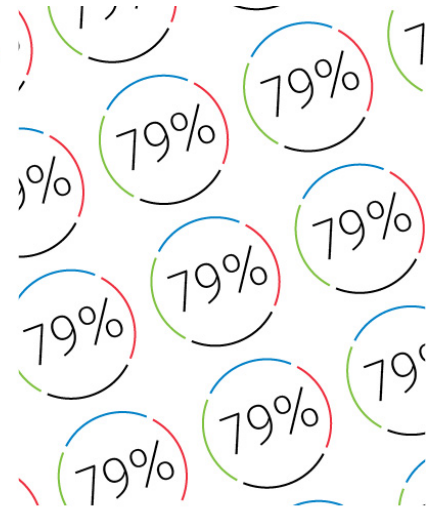
---

79% of the lawyers experience significant impact on their work as they are coping with increased volume & complexity of information.

**Discover how Kluwer Competition Law can help you.**  
Speed, Accuracy & Superior advice all in one.



2022 SURVEY REPORT  
The Wolters Kluwer Future Ready Lawyer  
Leading change



This entry was posted on Friday, December 15th, 2023 at 9:00 am and is filed under [Data Act](#), [Data protection](#), [Digital](#), [Digital competition](#), [Digital economy](#), [Digital markets](#), [Digitisation](#), [European Union](#), [Regulation](#)

You can follow any responses to this entry through the [Comments \(RSS\)](#) feed. You can leave a response, or [trackback](#) from your own site.