31 January 2023

Scenarios if the Data Act was already applicable

THE CASE FOR MORE CAUTIOUS DELIBERATIONS ON THIS REGULATION

Throughout the past months BusinessEurope and its members have made concerted efforts to showcase that the proposal for the Data Act, if done right, has a potential to make Europe a leader in the next wave of digital transformation. To this end, the provisions in this first of a kind regulation for Europe's industrial base must be founded on competitiveness-by-design. The examples[1] gathered below show the concerns of the industry in Europe when assessing the potential impact of the obligations on the ground.

****

Potential negative consequences due to unclear scope of "data":

In versions of the amended Data Act proposal, there are different terms introduced to clarify the types of data in scope, e.g.: "readily available data"; data that can be obtained without "going beyond a single operation"; "all data that the product generates as a result of user action… including in times of inaction, standby, switched-off … Datapoints automatically generated without any form of processing; prepared data, with metadata and context, combined or sorted data…"; etc. [Council, 4th compromise text, Article 2(1ae); Recital 14a].

Example: *Company "A"*[2] is a car manufacturer. Its vehicles generate and process various amounts of data within their internal components. However, not all data are (technically and legally) accessible for and used by the car manufacturer. Some data, for instance, are generated in components supplied by third parties to which the manufacturer has no access at all. If a car manufacturer needed to provide real-time access to data generated in a vehicle, this would require streaming and storage capacities way beyond current and foreseeable hardware settings in vehicles and backends of manufacturers.

Example: In the manufacturing industry, "*Company B"* typically has over 100,000 data points that feed into the line's automation system. About 10,000-20,000 measurement points measure raw physical data, which are combined with index and control values *(*and would qualify in one or more of the categories above*)*. The knowledge of which data from these measurement points are transmitted for processing could give knowledge to the data recipient how the machines are operated and even built, i.e., data related to the original equipment. *(Note that the data recipient, e.g., "Company C"*

[1] Non-exhaustive list. Document could be updated as new examples emerge.

[2] Names of the companies have been changed for reasons to protect their commercial status and business relationships.

may also be a direct competitor who may already manufacture similar or same products and provide a related service.)

In other words, because of the broad definition of data and the vast number of products and business models in scope, there is a high chance that in some instances "Company B" will be obliged to give to its direct competitor "Company C" sensitive knowledge about the original equipment. While this knowledge is not the subject of the contract for service provision between the User and the data recipient, the broad definition of data to be transferred may well capture it.

> **Insufficient measure**: The prohibition for *the "Company C" (data recipient)* to develop competing product based on the data it received, does not protect "*Company B"* 's investment in obtaining advantage on the product market. It must be highlighted that precisely because of this investment and advantage, "Company B" is the preferred choice of the User to purchase the product over the one from "Company C". The User only chose the latter for an aftermarket service.
>
> **Suggestion: Only raw data in scope, and leave the market to shape**
> The Data Act provides a possibility for the data holder to request compensation from the data recipient for making data available. Any "prepared", "cleaned", "contextualized", data the data holder "can obtain" etc. data will only increase the cost of making that data available, and henceforth the compensation requested. To avoid unnecessary costs and to enable the innovation capacity of all players, the scope should be limited to *raw data*. Furthermore, if the data recipient provides a service of value, which the User prefers, then the data recipient actively worked to be in that position, and it will have enough capacity to clean, prepare and make use of raw data, without the need for facilitation from the data holder.

Potential chilling effect on business models of niche products and services

Example: "Company D" builds data capabilities to their forest machinery. It creates data offerings and provides customers with relevant data. Data on performance of machines and components are being processed and shared downstream to component manufacturers. "Company D" has less than 5 000 employees, yet as a large enterprise it falls in scope of the Data Act.

A direct competitor of "Company D" has more than 10 000 employees. Having twice the size, the competitor could offer a cheaper service. Users may choose a cheaper service provider just as "a trial", yet the trial period will be enough for the competitor to obtain important data of the machine. Such scenario will have a chilling effect for a relatively smaller company that relied on innovative approach to challenge an incumbent.

> **Suggestion: Compensation with a profit margin and investment protection**
> A compensation merely covering the cost of making data available and without the possibility to establish a margin of profit for objective reasons, will inevitably drive niche products and services out of cash. We welcome Recital 41 of the proposal of Data Act stressing that "It is not unlawful discrimination, where a

data holder uses different contractual terms for making data available or different compensation". Recital 42a mentions that the margin of profit "may be limited or even excluded in situations where the use of the data by the data recipient does not affect the own activities of the data holder." However, it could be made clearer that margins can go higher if the data recipient's use of data affects the activity of data holder.

Furthermore, "Company D" designs the machinery with a data-generation possibility from the earliest stage and make investments in order to ensure that data can be used for a value-added service. Therefore, the Data Act should clarify that the *sui generis right* derogation is "without prejudice to the instances where the requirements for protection according to Directive 96/9/EC, such as the presence of proof for substantial investment, are met."

Potential impact of the global competitiveness of businesses in the EU

Example: On highly specialized machines, the level of knowledge among competitors is typically high. The competitive assets of the companies are based on attained extensive know-how and quite small differences not necessarily on technical capabilities but on fine-tuning the machines on the basis of data to get the abilities to produce, for example, paper for banknotes versus producing regular paper. These very small differences give some European companies the competitive edge over competitors from third countries that have basically the same technological capabilities but rely on bulk data only.

Example: In the clean energy sector, the situation is very similar. "Company E" and its subsidiaries in the corporate group have highly sophisticated systems and grids. The competitive edge comes from datasets and small differences attained by the group, for example, in improving electricity distribution and efficiency. Such knowledge could be exposed to third country service providers, with which "Company E" may even have previously not entered business relation.

Example: In the aeronautical industry, "*Company F"* communicates technical data on aircraft to other (trusted) companies for aircraft maintenance. This is essential to monitor temperature/pressure variations, wear, and tear of a piece, and make sure that the maintenance is done properly. If the User wants to switch to another service provider, there is no obligation for any due diligence process examining the origin, biography, track record, potential controversies, legal disputes, past or current behaviours of the competitor. By obliging the data holder to sharing data to (known or unknown) third country parties, the analysis of this data could make it possible to understand the functioning of the sensor or of a component of the aircraft and to make copies of it and compete with the data holder on third country's home market.

Suggestion: Build data flows based on trust and on contractual relationships

The examples above show that the User is by no means the owner of the company's competitive market advantage of the product or the service, yet the right of the User can force the sharing of strategic data, de-facto taking that competitive edge out of the hands of the data holder. The current wording of the Data Act does not provide any feasible nor fool-proof mechanism for European industry to enforce any "protection" of this competitive advantage. When

advancing data flows in industries, it is best to build it on existing contractual relationships and trust.

Switching data processing service providers must support the agency of the User

Example: Chapter VI does not seem to sufficiently acknowledge that a *"User X"* is the one who voluntarily decides to switch service providers, which is a (informed) decision after reviewing and comparing different offers of multiple providers and considering its specific needs. Instead, somewhat by presuming what a *"User X"* wants or needs, the text in Chapter VI establishes detailed obligations to the original/source cloud providers, on how to technically enable the switching, what periods to abide to, types of data to be ported, etc. The level of detail to such intervention may have unintended consequences for the market, which currently takes-up voluntary codes of conduct to enable switching and porting, such as SWIPO. The European Commission states that its SWIPO evaluation *"exclusively adopts a legal perspective;"* and that the procedural aspects regarding the self-regulatory process and market uptake of the codes of conduct *"are not covered".*[3] Considering this limitation of the Commission's evaluation, the provisions of Chapter VI need more careful examination for their potential impact on contractual freedom, the free choice of "User X", and the cooperation dynamics between the market players.

Suggestion: Avoid detailed obligations and strengthen the User's agency

An unintended consequence of detailed obligations for the service providers may, in effect, render the switching process less costly for established providers than for market challengers. Therefore, the User, the source, and the destination data processing service provider must cooperate and have the flexibility to tailor the switching process according to the needs of the User, while respecting the legal obligations any of the involved data processing service providers may be subject to; obstacles that amount to vendor-lock-in and user's inability to port data must be removed. This way contractual freedom is preserved, the market has a breathing space to evolve and innovate; it will not stifle market challengers with too prescriptive obligations, and at the same time User's right to port data is secured.

This non-exhaustive list of examples from different industries in Europe shows the vast impact of the Data Act. Overthinking the Data Act may not be politically attractive but underthinking it could have a chilling effect on Europe's industrial potential, and lead to data *desertification.* In this respect, it must be recalled that another comprehensive legislation that set Europe apart and became a blueprint globally - the GDPR - was discussed over four years and is still maturing[4]. If the Data Act has to replicate the

[3] Study presenting assessments of codes of conduct on data porting and cloud switching

[4] The European Commission released the GDPR proposal in January 2012. The European Parliament adopted its position on 12 March 2014. The Council achieved a general approach on 15 June 2015. The adoption of the new data protection framework took place on 14 April 2016 and made it applicable as of 25 May 2018.

same effect and become a global standard, there is no evident reason why this regulation should take less time to be negotiated.