Kluwer Competition Law Blog

Data Marketplaces and the Data Governance Act: A Business Model Perspective

Santiago Andrés Azcoitia (IMDEA Networks) and Alba Ribera Martínez (Deputy Editor) (University Carlos III of Madrid, Spain) · Monday, September 18th, 2023

The data economy is now thriving. A considerable corporate, entrepreneurial and research effort is aimed to enable a healthy trading of such an important asset, and hence contribute to de-siloing data and unlocking the combinatorial economic value of data that now rest in different corporate warehouses. However, the structuring of data ecosystems is still under development. Following research we performed, data markets are moving away from traditional horizontally integrated monolithic data providers, and towards distributed '*niche*' exchange platforms, through commodifying and specialising data sharing.

The Data Governance Act sets up a harmonised framework for the development of trustworthy data intermediation services in the Union to enable a competitive environment for data sharing. This instrument requires data intermediation service providers to be neutral with regard to the data that are exchanged, the data holders, the data subjects, and the data users. It establishes the obligation for data intermediation service providers to be registered as an *EU Recognised Data Intermediary* and the conditions they must fulfill to do so.

Such conditions are not necessarily aligned with some of the trends observed in the market, which may create friction in applying and enforcing the Data Governance Act. In this post, we highlight some of these points of friction and discuss some derived challenges that competent authorities (these may be data protection authorities, according to the co-legislators) for data intermediation services will face when interpreting and applying the DGA in the current market.

The business models of entities trading data in the B2B market

Unlocking the value of data as an essential production factor of the economy has become a cornerstone of ICT and digital policies all over the world. In the EU, Building a European Data Economy and the European Strategy for Data are key pillars of the European Digital Decade overarching policy.

Different actors have entered the market to facilitate the exchange of data between potential users and data holders. Even though most publications loosely refer to them as *data marketplaces*, they resort to different business models (as shown by our recent empirical research in the field).

Basically, there are three types of business models which one can differentiate depending on the purpose and targets of the data exchange; i) those business models providing data and services to their users (data and/or service providers); ii) those business models mediating data transactions between data holders and data subjects (data marketplaces); and iii) those business models that facilitate data management to then transact with third parties (data management systems).

Data providers (DPs) and *Service providers (SPs)* are both entities providing data products or digital services to end users, be they individuals or enterprises, based on data they own, they collect from the Internet or infer from their data sources. Whereas data providers directly cater data for their users, service providers cater integrated services mediated by the use of this data. Both types of operators collect data from the Internet or acquire them from third parties. By scraping data from the Internet we found more than 2,100 DPs cater for many different types of data, ranging from financial to marketing services, including weather or gaming data.

BookYourData is an example of DP offering contact lists of individuals or companies in the US, and Hexagon acts as a DP when it offers access to its database of satellite imagery data.

Clearview.ai is a controversial example of a SP, given that it provides identity data based on pictures of people publicly available on the Internet. Not without any backlash, the European Parliament condemned in late 2021 the company's activities in the EU, mainly as they were being applied to contexts where grave interferences were being caused vis-à-vis the exercise of fundamental rights, namely for mass surveillance in the exercise of behavioural policing and society scoring. The newly proposed (and yet ongoing within the legislative process) draft regarding the use of Artificial Intelligence (AI Act) may prohibit entirely scraping activities for the purpose of biometric identification when they are deployed indiscriminately.

Interestingly, the boundaries between DPs and SPs are often blurry. Clearview.ai delivers the existing connections between pictures to biometric identities in the end, which are in itself data, and so it might be considered a DP. However, they do not deliver mass datasets but more complex facial recognition services based on data they own and process which is why we consider it to provide services.

Data Marketplaces (DMs) are mediation platforms that put providers in touch with potential buyers and manage data exchanges between them. Such exchanges usually involve some kind of economic transaction (either through payments in fiat currency or in a cryptocurrency often created and controlled by the platform). DMs are either public – i.e., open to any data seller or buyer – or semi-private, meaning any seller or buyer is subject to the approval of the platform in order to be allowed to trade data. Furthermore, DMs often deal with data categorisation, curation, and management of metadata to help buyers discover relevant data products.

Data Management Systems (DMSs) are platforms that make catalogs and help with data governance of large enterprises and corporations. They are increasingly offering add-ons to carry out secure data exchanges within an organisation and to enrich its corporate information base by acquiring data from second or third-party providers.

Within the broader category of DMSs, in the retail market *Personal Information Management Systems (PIMSs)* empower individuals to take control of their personal data and act as a single point of control to manage them. They leverage recent data protection laws (GDPR, CCPA, etc.) so as to let users collect personal information controlled by digital service providers, exercise their

erasure or modification rights as granted by law, manage permissions of mobile apps to give away their data, manage cookie settings, etc.

Some entities only implement specific functions of data sharing, which they offer to DMs, PIMS, or DMSs. Such *enablers* provide a range of solutions that include, for example, anonymizing personal information (AirCloak), providing a homogeneous anonymised identity to buyers (Datavant), facilitating secure exchanges (Cybernetica), or empowering individuals to exert their rights on the information that data providers hold about them (Saymine).

Market challenges and trends

Even though there is an ongoing titanic effort both from governments, industry and academia to develop the data economy, some relevant challenges still prevail and hinder data markets. Key challenges were found related to their fragmentation and the lack of standardisation, data valuation and pricing, transparency of data markets, data ownership, and tracking data provenance.

Against this background, the data-sharing market is becoming more and more specialised, with general-purpose data marketplaces being replaced by niche platforms. Moreover, data exchange is somehow becoming a commodity, with many different actors found to be adding and sharing marketplace functions to complement their business core operations.

Data Intermediation Services

Aside from the categories we have presented above, the Data Governance Act (DGA) defines "*data intermediation services*" as those services aimed to establish commercial relationships for the purposes of data sharing through technical, legal, or other means between data subjects and data holders on the one hand and data users on the other. The definition explicitly excludes services related to copyright-protected content, services that focus on one party only (e.g., curation of data for a data provider), and non-commercial data-sharing services offered by public sector bodies (Article 2(11) DGA).

Most entities trading data in the B2B market are covered by this definition of data intermediation services, and therefore are affected by the new Regulation. A recent report by the European Commission's Joint Research Group identifies six types of data intermediaries that include DMs and PIMS, in addition to data cooperatives, data trusts, data unions, and data sharing pools.

Data cooperatives are entities that aim to improve data governance of a community (of individuals or companies) and increase their control over their information by observing agreements between their members to share, process, and use their data. In a *data trust*, the *trustee* agrees to manage and take care of the data rights of its beneficiaries, who also benefit from the pooling of their data and the economies of scale this generates. *Data unions* are associations of workers and users of digital platforms and services that aim to defend their interests in the use the latter make of the data they produce. Finally, *data sharing pools* are alliances between data holders to share, process and use their data jointly pursuing a shared purpose or application.

According to the DGA, data intermediation services providers (DISP) shall meet a number of

obligations, such as the need to notify and register to obtain the label of *EU Recognised Data Intermediary* and provide data intermediation services through a separate legal person.

Stemming from the catch-all definition provided in Article 2(11) DGA, DISPs connect individuals/companies with data users in a *neutral* manner. In this regard, they are aimed at fostering trust in data-sharing, which has been highly undermined in the past. Thus, DISPs are only reduced to their role as intermediaries acting in the best interests of the data holder and not using the exchanged data for other purposes.

A different regulatory approach to the rest of harmonising instruments of the Union

Unlike the Union's Digital Markets Act (DMA) and Digital Services Act (DSA), the DGA applies to all data intermediaries willing to provide DIS in the EU and they are subject to the terms and conditions of this regulation, notably to Articles 9 to 14. At one extreme of the verticality of regulation, the DMA applies only to those operators (now recently designated, see review here) addressed as gatekeepers due to their relevance in the artificially tailored core platform services that the DMA introduces into the regulatory space.

In an intermediate position, the DSA applies to all providers of intermediary services, but it compels the providers of online platforms and search engines (and especially very large ones) to harsher obligations. These intermediary services are not to be conflated with data intermediaries under the DGA, insofar as under the DSA intermediary services relate to those operators catering for information society services via conduit, caching or hosting services (Article 3(g) DSA). Online platforms and online search engines are categorised within the DSA as types of intermediary services catering for specific services to end users. At the same time, these definitions steer clearly away from the definitions of core platform services contained under Article 2 of the DMA.

Irrespective of the fact that the three instruments (alongside the draft Data Act which is also taking its twists and turns in terms of trilogue negotiations) are based on the same tending-to-harmonisation legal basis, i.e., Article 114 TFEU, they are set apart miles away from each other in terms of their scope, substance and the timeframe which is set out for compliance as far as their data-related obligations are concerned.

In terms of the immediate actions expected from the operators, the DMA is the most lenient (but arguably the most transformative) instrument with the targets of the regulation, insofar as a 6-month period is placed as the first landmark for compliance but, in any case, a fully-fledged manifestation of instantaneous compliance with the substantive provisions is not expected as early as March 2024. Compliance will be a work in progress, stemming from the gatekeeper's and Commission's encounters and interactions. Regarding the DSA, very large platforms and online search engines are expected to adjust their behaviour online in the period of four months, including undertaking and providing the Commission with a first risk assessment. As opposed to both of them, the DGA's provisions are already fully applicable and have been since early September (whereas the DISPs already in operation have until 2025 to comply).

The overarching policy objectives of each instrument are also different. The DMA and DSA clash in terms of the private rule-making that they want to bring down in favour of levelling the playing field in economic terms and in securing a safe, predictable and trustworthy online environment

where Union citizens may exercise their fundamental rights. In the particular case of the provisions surrounding data intermediaries under the DGA, the overall objective is not to contest the power of Big Tech, but rather to establish an alternative model to Big Tech platforms that hold a significant degree of market power (Recital 22). By this token, data intermediation services are aimed at indirectly creating a more competitive environment (Recital 33).

The DGA creates friction in the market

In light of the above, it is interesting to note that the market is not necessarily heading in the direction pointed to by the new European legislation. This will surely create some friction in applying the DGA to global firms that are already providing data-sharing services over the Internet.

For example, some data marketplaces complement already-existing data-driven services in some flourishing business models. For example, SPs like the so-called '*data-brokers*' (Liveramp, Lotame, Openprise, among others) are adding private marketplaces into their platforms to allow secure exchanges, monetisation, trading, and integration of audience data. GIS platforms like Carto or Here are adding data marketplaces for their users to acquire geospatial data intended to be used within that system. Enterprise DMSs are embedding secure data exchanges within the walled garden of information under the control of each customer, and data marketplaces to bring (some of) these data assets to the market. All of them are offering data sharing somehow tied to another service, which reduces the risk of bootstrapping a data marketplace from scratch but may contravene the neutrality rationale required by the DGA.

Furthermore, most data products currently offered in DMs do not show fully transparent pricing terms to potential customers, but they start by asking their identity or the purpose they want to use data for in order to quote (and customise) the data product. This might directly contradict the spirit of Article 12 of the DGA. Moreover, establishing a sound concept of *fairness* in pricing data products, which are easily versionable in many different ways, will probably become a great challenge for competition economics (as it has been in the area of patent licensing, and as it is expected to be when applying the DMA's FRAND obligations, see Colangelo's work in this regard).

Interpreting the DGA is key

From a technical perspective, defining appropriate levels and responsibilities in securing data at rest and on the move is also one of the most salient challenges in securing DGA compliance. In this respect, we are witnessing European initiatives heading in different directions. On the one hand, the DGA imposes important security responsibilities to DISPs (e.g., the maintenance of activity logs, obligations regarding security and fraudulent practices, etc.). On the other hand, some European standards like IDSA and the Gaia-X project are already defining and developing mechanisms to secure data exchanges, and so is a thriving group of start-ups like Ocean Protocol. Still, the elusive nature of data makes it very hard to achieve bullet-proof security even with cutting-edge technology in the field, and hence interpreting the DGA to define what DISPs must do and what they cannot do when fighting against unauthorised data breaches will also be crucial.

Competent authorities for data intermediation services will have to deal with these issues when applying the DGA and assessing the DISPs eligible to become *EU Recognised Data Intermediaries*. And this interpretation will also be key in ensuring the success of data marketplaces, PIMS, and other data intermediaries in the Union.

To make sure you do not miss out on regular updates from the Kluwer Competition Law Blog, please subscribe here.

This entry was posted on Monday, September 18th, 2023 at 9:00 am and is filed under Data protection, Digital competition, Digital economy, Digital markets, Digital Markets Act, Digital Services Act, 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.