BLOMSTEIN

DMA and Data
No More Leveraging for Gatekeepers?

19 March 2024

Since March 7th, all core platform services that the European Commission has designated as gatekeepers under the Digital Markets Act (DMA) so far, must comply with the DMA's obligations and had to submit comprehensive compliance reports. In these reports, they must show in a detailed and transparent manner all relevant information needed by the European Commission to assess the gatekeeper's effective compliance with the DMA.

In our series of briefings, we recap the key milestones of the DMA implementation, deep dive into the various obligations that gatekeepers are facing, lay out the DMA's implications for stakeholders who are not (currently) within the direct scope of the legislation and update you on the current status of affairs in the DMA's implementation.

This time we focus on: Data related DMA obligations.

Data Collection and Market Power

At its core, the DMA addresses the crucial issue of data and market power, aiming to redefine gatekeepers' rights and responsibilities when collecting data from business users and end users. By establishing rules on the processing, combination, and utilization of data, the DMA aims at restraining the ability of gatekeepers to leverage their control over vast datasets sourced from core platform services to assure market dominance across multiple data driven markets where these data sets provide the gatekeeper a competitive advantage.

Picture this: You are an online retailer using a gatekeeper's marketplace. The gatekeeper competes with your business at the retail level and takes advantage of data obtained from your sales and customers in the marketplace. Further, you are an ad-tech company who uses a gatekeeper's social media platform to launch advertisement campaigns. The gatekeeper uses personal data derived (e.g., clicks, views) from the campaign to feed its data base for the provision of advertisement services itself. Or you are a provider of software applications which uses a gatekeeper's software application store. The gatekeeper uses data derived from your business' activities in the application store to inform decisions related to its own offering of software applications. These scenarios depict some of the business practices the DMA aims to prevent as the default practice of gatekeepers.

Limiting Data Leverage, Reinforcing Data Privacy

Article 5(2) of the DMA imposes stringent limitations on the conduct of gatekeepers concerning the accumulation and use of end-user data. Gatekeepers are now required to refrain from the following behaviours, unless the end-user provides express consent:

> (1) processing personal data sourced from third parties (e.g., business users) for online advertising purposes,
>
> (2) combining personal data sourced from the core platform with data sourced from other services provided separately by the gatekeeper or from third-party services,
>
> (3) cross-using personal data sourced from the core platform service in other services provided separately by the gatekeeper,
>
> (4) signing-in users to other services of the gatekeeper to combine data.

This provision builds upon the framework established by the General Data Protection Regulation (GDPR) and broadens its principles to encompass potential market distortions. By doing so, it not only grants individuals more control over shaping their online experience according to their preferences, but also seeks to promote the contestability of core platform services by enabling end users to freely choose if and how a gatekeeper uses their data. The DMA recitals expressly indicate that access to core platform services or certain functionalities shall not be conditioned to the end user's consent. Therefore, a less personalised service should not be different or of degraded quality compared to the service provided to the end users who provide consent.

In fact, the concerns addressed in this provision evolve from previous case law. In 2019, the German *Bundeskartellamt* found that Facebook breached competition rules by compelling users to agree to the combination of their social network data with personal data collected from other Meta services such as WhatsApp and Instagram (see decision here). This understanding was later confirmed by the European Court of Justice (Case-252/21).

Notably, Meta has taken steps towards compliance with the GDPR and the DMA by introducing an advertisement-free subscription option for Facebook and Instagram. However, it remains to be seen if it is an acceptable business solution to assure compliance with this DMA provision.

Safeguarding Business User Data

Article 6(2) focuses on the relationship between gatekeepers and their business users, mandating that gatekeepers refrain from making use of non-public data sourced from business users to directly compete against them in an adjacent market (e.g. online retail,

advertising, software applications). The provision aims to foster a level playing field wherein businesses are not unfairly disadvantaged by the platforms they rely on.

Non-public data encompasses various forms of information, including both aggregated and non-aggregated data derived from the commercial activities of business users or their customers. This includes data directly related to the business, such as suppliers, prices, orders, terms and conditions, as well data related to the customers of those business users, such as clicks, searches, views, and voice interactions, occurring within the core platform services or ancillary services provided by the gatekeeper.

This provision also draws from past case law notably exemplified by the investigations involving Amazon conducted by the European Commission and the CMA. The focal concern was Amazon's potential utilization of non-public business data sourced from marketplace sellers, which could enable its retail arm, Amazon Retail, to optimize decision-making processes, e.g., identifying lucrative product markets, engaging directly with successful suppliers of third-party sellers, and negotiating supplier terms more favourably. These investigations resulted in commitments from Amazon to abstain from employing such data in its retail operations.

Comprehensive Implications for the Digital Ecosystem

The implications of these provisions are far-reaching across the digital ecosystem:

- For gatekeepers: The provisions require a fundamental reassessment of how user data is collected, processed, and used. Compliance will require technological and procedural adjustments, such as most obviously the introduction of a consent prompt, and potentially also altering business models where user consent cannot be acquired.
- For third-party business users: The provisions offer a safeguard against core platform service providers leveraging data sets across their ecosystems that have been collected with the help of third-party business users. Breaking open the walled gardens many gatekeepers have been building (e.g. through the all too convenient single sign-on) may establish a more equitable level playing field for third-party business users.
- For end users: Promise a more user-centric digital environment, with enhanced privacy protections and a wider choice of services. On the other hand, sceptics question the practical effects of the opt in provision, noting the challenge for end-users to fully grasp the implications of sharing their data, thus hindering their ability to make an informed decision when deciding whether to provide consent.

Looking Ahead: Enforcement

By tackling the complex interplay between data and market dominance, the DMA data provisions are a key enforcement tool with an ambitious mission: Rebalance the data value chain by limiting how gatekeepers collect and use data. Through this effort, the aim is to cultivate a fairer landscape for competitors in data-driven markets by limiting

how gatekeepers make use of data sets across the various services they provide. However, in particular in relation to Article 5 (2), the actual potential to bring about the desired change in the competitive dynamics of the digital markets highly depends on end users making thoughtful use of their newly acquired consent rights. Where end users out of convenience consent, a phenomenon well observed in relation to cookie consent banners, the DMA provision is at risk to remain a toothless tiger.

In fact, business partners of gatekeepers, competitors and consumer organizations play a significant role in the enforcement of these provisions. The DMA introduces relevant tools and opportunities for third-parties to flag ongoing misconducts and assert their rights, e.g., presenting complaints to the European Commission or National Competition Authority (NCA), applying for interim measures before the European Commission, and seeking injunctive relief and damages in national courts (see our briefing on private enforcement of the DMA here).

BLOMSTEIN will continue to monitor and assess the developments and practical application of the DMA provisions. If you have any questions on the topic, Anna Huttenlauch, Elisa Theresa Hauch and Ana Carolina Vidal will be happy to assist you.