BLOMSTEIN

Data on Demand? Access to Gatekeeper data for business users under the Digital Markets Act

23 April 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 on: Real-time access to gatekeeper data for business users under Article 6(10) DMA.

Uneven Access to Platform Data

Imagine an e-commerce company engaging with customers through a third-party online marketplace. The company has limited access to customer and transaction data through the marketplace's B2B interface. However, the bulk of the generated data remains with the operator of the marketplace. Now suppose the company wants to migrate its customers elsewhere, perhaps to its own web shop or another third-party platform. The data gap is likely to widen: Most customer data and information generated through the marketplace will remain with the operator of the marketplace and cease to be available to the company. However, if the original marketplace qualifies as a core platform service and its operator as a gatekeeper within the meaning of the DMA, the e-commerce company may have a way out in the future.

The DMA is designed to curb data-driven advantages that "big data" companies allegedly enjoy over their competitors. In a previous briefing, we discussed how the DMA seeks to restrict the ability of these gatekeepers to leverage non-public data sourced from business users to compete directly with them in adjacent markets. This time, we look at the other side of the coin: how businesses can use the DMA to gain **permanent real time access to data** relating to their use of core platform services.

The Goal: Dissolving Data Silos through Access Rights

Many businesses rely on platforms or intermediary services provided by digital gatekeepers. These services provide reach and make it easy to connect and transact with customers. In the process, both businesses and customers provide and generate vast amounts of data, both knowingly and unknowingly. This includes data on transactions, user preferences, payment settings, reviews, ratings, and even sensible personal data such as names, age, gender, shipping and IP-addresses. These data sets are highly valuable. Gatekeepers can use them to enhance their own services or gain competitive insights. They could also help businesses refine their products or marketing strategy. In practice, however, often only the gatekeeper has full visibility. For business users, these 'data silos' can limit insight into customer behaviour and create barriers to migrating customer data or multi-homing competing platform services in parallel.

The DMA intends to address these data silos and perceived data-driven imbalances. To level the playing field between gatekeepers and their business users, Article 6(10) DMA grants the latter access rights to data related to their use of core platform services.

Extent and Limits of Data Access under Article 6(10) DMA

Article 6(10) DMA gives business users the right to request from gatekeepers *free of charge, permanent real-time access to data* provided for or generated by them and their customers in the context of the use of the relevant core platform services. This right extends to data related to services provided together with, or in support of, the core platform services by the business user or the respective customers. In a nutshell: Business users can request access to the data package generated by their commercial activity via a core platform service.

Article 6(10) DMA sets out various requirements for data access:

- **Explicit request:** The gatekeeper is obliged to grant data access only upon request of the business user (or third parties authorized by the business user).

- **Provided or generated data:** Generally, the access right includes the complete digital data package attributable to a business user - irrespective of data type. This includes data in the form of audio, visual or audiovisual material, potentially even tracking data such as search behaviour, clicks, views, location data and raw data that can be further processed. The gatekeeper must grant the business user access to both aggregated and non-aggregated data. Apart from data voluntarily provided by users, this includes observed data such as clickstream, search and raw data. However, access rights do not cover derived data entirely created by the gatekeeper itself based on provided or generated data. In many cases, it will be challenging to distinguish derived gatekeeper data from merely observed, reformatted or aggregated data.

- **User consent for personal data**: Access rights extend to user personal data, provided it directly relates to products and services offered by the business user via a core platform service. However, disclosure of personal data requires effective consent from the customer and must comply with privacy laws, particularly GDPR requirements. The necessary consent (tacit or explicit) should often already exist, as the relevant data was specifically provided or generated by customers for utilising products or services of the business user. Where consent has not yet been given, gatekeepers may need to allow customers to opt-in to data transfers.

- **No third-party data:** Data portability obligations only cover data provided or generated by the respective business user or corresponding end users. There is no obligation concerning third party data. To the contrary, access to competitor data, for instance, could potentially violate competition law or protected business secrets and entail a risk of fines.

- **Link to core platform service:** Data is only covered if provided for or generated in the context of the use of a core platform service or services provided by the gatekeeper together with or in support of these. Data sets provided for or generated in the context of other, unrelated services of the gatekeeper are not covered.

- **"Free" access:** Data access must be "free of charge". The gatekeeper may not make access conditional to (direct or indirect) fees or other commercial conditions that could prevent business users from accessing them. As such, gatekeepers will not be able to directly pass on compliance costs to access applicants. For instance, they will likely not be able to claim compensation for software licenses, electricity costs or staff working hours. Gatekeepers could, however, request reimbursement for formatting data in a specific format, provided the relevant data sets are alternatively offered in a standard exportable format for free. Compensation is also conceivable for obviously unfounded or excessive requests, i.e. access demands outside of the scope of the DMA.

- **Effective and high-quality access:** Gatekeepers are required to provide "effective" and "high quality" data access. Effective means that access must be facilitated in a way that enables comprehensive and tamper-proof electronic retrieval of the data. This requires gatekeepers to implement "appropriate and high-quality technical measures", such as specific APIs for real-time data access, or, if necessary, offer different levels of aggregation required for data portability. The DMA considers access as "high quality" if it is "state of the art", user-friendly and possible at a reasonable level of effort.

- **Permanent real-time access:** Finally, data access must be "real-time" and "permanent", meaning the gatekeeper must ensure data retrieval at any time and on

an ongoing basis. For instance, access must not be tied to business hours or deadlines set by the gatekeeper. Also, real time changes to the data package must be visible in the data sets accessible to the business user without significant delays: business users must be given access to the current data status and be able to use or export their current data package at any time. Here too, the DMA refers to the possibility of establishing APIs.

When can Gatekeepers Refuse Requests for Data Access?

Data access for businesses under Article 6(10) DMA is limited to core platform services provided by gatekeepers. This means that companies will only benefit from enhanced data portability from a very limited number of designated companies - and only in relation to a subset of their respective services.

In addition, gatekeepers may deny requests for access to data sets protected by intellectual property rights or containing trade secrets. However, data generated or made available by business users and their respective customers when interacting through core platform services will rarely contain trade secrets vis-à-vis the business user. As the party responsible for ensuring effective access, the gatekeeper must take suitable measures to provide ensure data is not linked to business secrets or IP rights. This could be done by structuring or aggregating the data accordingly. In practice, gatekeepers will therefore rarely be able to prevent data access by invoking IP rights.

Other than that, the gatekeeper may only refuse access requests in exceptional cases, such as obviously unfounded or excessive requests. For example, a gatekeeper may refuse access requests or demand cost compensation for repeated isolated requests from businesses, provided that a viable alternative option for permanent real-time access exists. Whether a particular request is abusive or excessive will have to be assessed on a case-by-case basis.

Implementation and Enforcement: Plenty of Space to Fill

The DMA's rules on data access for business users leave room for interpretation, their practical implementation could lead to disputes. Many aspects require clarification: at what point is access really "high-quality?" What downtimes are acceptable for "permanent" access, e.g. in the event of technical adjustments or updates to core platform services? How can gatekeepers effectively protect IP and trade secrets without jeopardising effective access? When is data sufficiently linked to core platform services to be eligible for access? To what extent will gatekeepers have to reformat or compile context-specific and difficult data to ensure transferability? And lastly, since Article 6(10) is intended to facilitate multi-homing and data portability, can gatekeepers reject access requests if businesses demand data access for reasons not intended by the DMA or even contravening its procompetitive rationale?

It is expected that the EU Commission will issue **guidelines** or adopt **implementing acts** to regulate the form, content and details of technical measures to be taken by gatekeepers pursuant to Article 6(10) DMA. In addition, the EU Commission can mandate European standardisation bodies to develop suitable standards for the technical implementation for data access. However, the main responsibility (and at the same time a considerable amount of autonomy in terms of technical implementation) will initially lie with the gatekeepers.

In the event of non-compliance with the gatekeeper's obligation under Article 6(10), the EU Commission may, inter alia impose **fines, periodic penalty payments and interim measures**. In addition, the DMA lends itself to private enforcement. Since Article 6(10) gives business users a direct claim against the gatekeeper, national courts are likely to play a role in defining access obligations. German competition law, for example, was amended in 2023 to explicitly allow damages claims based on DMA violations.

Conclusion

Data access for business users under the DMA could have significant implications for e-commerce and the digital ecosystem:

- *For end users*, immediate changes are unlikely to be very noticeable. They will mainly concern consent and data portability option, and, indirectly, potentially more frequent changes in distribution channels and platforms used by the companies they use. Depending on one's perspective, this could either lead to more choice and privacy for consumers – or further complicate digital consent requirements with little practical benefit.

- *Businesses* should now examine whether they can benefit from the data portability promised by the DMA. First, they should identify which of their business partners are gatekeepers. They should also assess whether they source B2B-services that qualify as core platform services. In addition to online marketplaces, this could include app stores, online search engines, social networking services, messaging services, video sharing platforms, virtual assistants, web browsers, cloud computing services, operating systems, and advertising services. On this basis, businesses should consider whether they can use data access rights granted by the DMA to enhance their own data pool - e.g. for later customer migration.

- *Gatekeepers*, on the other hand, need to ensure that an effective and robust mechanism for handling data access requests is in place. Compliance with the DMA may require technical adaptations to enable user consent, and possibly also the modification of business models where user consent cannot be obtained. At the same time, however, gatekeepers should be equipped to identify and defend against unauthorised, unsubstantiated or abusive access requests.

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 Philipp Trube will be happy to assist you.