Exploring the rules and requirements of the Digital Markets Act

11 November 2024

The Digital Markets Act (DMA) is a groundbreaking piece of European legislation designed to level the playing field for companies operating in Europe's digital market by limiting the dominance of large online platforms. By using pre-defined criteria to designated large online platforms as "gatekeepers" and impose rules on them, the European Commission ("Commission") aims to create a more open digital environment.

What's the objective of the Digital Markets Act?

The Commission seeks to make the digital market more competitive for companies and safer for users. To do so, it has begun to implement a series of regulation designed to reduce the power accumulated by a small number of large tech companies over the past decade. With the DMA, the Commission seeks to increase consumer protection while limiting the control that these "gatekeepers" have within Europe's digital economy.

The Commission can designate a company as a gatekeeper if it provides certain digital services—so-called core platform services (CPSs)—and meets a set of criteria laid out by the Commission. As of August 2024, the Commission has designated seven companies as gatekeepers of 24 CPSs, including Alphabet, Amazon, Apple, Booking, ByteDance, Meta and Microsoft.

By imposing a list of obligations—must dos— and prohibitions—must not dos—on these large platforms, the DMA works to increase competition and innovation among businesses and improve choices, quality and prices for users.

Who does the DMA benefit?

The DMA aims to ensure fair competition by curbing the dominance of large online platforms and ensuring that smaller businesses have a fair chance to compete. The Commission believes that a fairer market landscape will encourage innovation and allow new ideas and businesses to thrive.

As a result of this competition, the Commission hopes that digital consumers will benefit from better choices, quality and pricing for products and services. It also hopes that the legislation will increase the trust and accountability of large online platforms by enhancing the transparency of their data practices and associated algorithms—further protecting and benefiting consumers.

The regulation intends to stop gatekeepers from locking consumers into their platforms and to make it harder for them to track users' internet activity and profit off this and other data they provide. In effect, it should increase access for businesses and consumers using the gatekeepers' CPSs while making it more difficult to gatekeepers to collect data on users and their activities.

Under the DMA, gatekeepers must offer users a choice of operating systems and web browsers, allow them to uninstall preloaded apps and make instant messaging systems interoperable. They can no longer force app developers to use only their tools or services or restrict them from offering better terms and prices on other platforms.

Gatekeepers will also have to become more transparent about their practices; for instance, they cannot rank their own products or services higher than those of third parties using their platforms, and they must gain explicit consent from users before tracking their activities for advertising purposes.

By introducing new rules around processing, combining, sharing and using data, the legislation strives to prevent gatekeepers from using the vast data obtained through their USPs to maintain their market dominance and place limits on user's choices and behaviour.

What are a gatekeeper's obligations and prohibitions under the DMA?

The DMA has far-reaching implications for companies designated as gatekeepers. Below is a summary of some of the major requirements:

Data governance

01 Data usage

A gatekeeper cannot process, combine or cross-use an end user's personal data on its other CPs for online advertising purposes unless the user provides clear consent. If gatekeepers obtain private data from a business using their platform, they cannot use that data to compete against the business.

02 Data sharing

A gatekeeper must give businesses using their CPSs access to important data, such as data about customer interactions and behaviours, to enable those businesses to better understand their consumers.

03 Data portability

At the request of an end user, a gatekeeper must provide them with their data, including both data the user provided to the platform and data generated by the user's activity on the platform (interactions, history, preferences, etc).

The gatekeeper must share the data in a way that makes it easy for the user to transfer it to another platform or service, providing the user with control over their data and making it possible for them to switch to another service without losing important information.

04 Data access

Users must be able to retrieve their own information quickly and easily, so a gatekeeper must permit both businesses and individual users to access any data they've provided to or generated without obstacles or delays.

Gatekeepers of search engines must also share important data—such as rankings, commonly searched questions and click rates—with competitors, in a reasonable way so that the sharing does not give any competitor an unfair advantage.

Access and choice

- **Most-favoured Nations (MFNs) Clause:** A gatekeeper cannot impose a wide or narrow MFN clause. As a result, gatekeepers can no longer lock businesses into unfair pricing strategies by requiring them to sell their products at the same or better prices than those offered on other platforms or their own website.
- **Interoperability:** A gatekeeper must allow products and services provided by other companies to connect and work seamlessly with its hardware and software. Gatekeepers of messaging CPSs must ensure that the basic functionality of their apps can work with similar services, thereby enabling users to communicate across different platforms and not just within the gatekeeper's ecosystem.
- **Access:** A gatekeeper must allow users to install and use apps or app stores from other platforms, giving users the flexibility to use products and services beyond what the gatekeeper offers and leveling the playing field for developers of competing apps by ensuring that their apps can be installed and accessed on a gatekeeper's platform without unfair restrictions.
- **Anti-steering:** Gatekeepers can no longer restrict businesses from promoting products and services on other platforms, and they cannot prohibit businesses from finalising sales or contracts with customers outside of their platforms. Gatekeepers must let businesses interact freely and directly with customers through other channels. For example, a gatekeeper must let a business promote a product on their CPS and still allow the business to direct customers to its own website where it offers better prices or conditions.
- **On-platform use:** If a user purchases a subscription, content or any other product from outside the gatekeeper's platform, the gatekeeper must still allow the user to access those features within the business's app. For example, if a user purchases an e-book directly from a bookstore's website, a gatekeeper cannot prevent the reader from reading the book within the bookstore's app. As a result, a gatekeeper cannot use its dominance to force a business to sell exclusively through its platforms.
- **Tying:** As part of the conditions for accessing services on its CPSs, a gatekeeper cannot force users to use its other offerings, such as web browsers or payment services. It cannot require users to subscribe to or register for its other services as a condition for platform access. Gatekeepers can no longer bundle their services within their platform in ways that prevent users from accessing alternatives.
- **Configuration choice:** A gatekeeper must allow users to easily uninstall software from its operating systems; change default settings in operating systems and web browsers that direct them to the gatekeeper's products and services; and give them the option to choose their preferred default search engine, web browser and virtual assistant.

Transparency

- **Self-preferencing:** A gatekeeper cannot treat its own products or services better than those of third parties using its platform. It cannot favour them in search rankings, indexing or crawling. Furthermore, a gatekeeper must apply clear, fair and non-discriminatory criteria for how it ranks, indexes and displays all products and services, ensuring that third-party services and products receive equal visibility and opportunity to compete with a gatekeeper's offering.
- **Transparency:** A gatekeeper must provide advertisers and publishers with detailed information about how it uses their advertising services and how it handles their payments. Gatekeepers must provide these stakeholders with visibility into the management and payment process for advertisements and be accountable for conducting their advertising practices in a fair and transparent manner.
- **Notification of mergers and acquisitions:** If a gatekeeper plans to merge with or acquire another company that provides digital services or collects data, it must notify the Commission even if the deal doesn't meet the usual thresholds for a merger review under EU Merger regulation. The notification will not automatically trigger a merger control review, but it provides the Commission with insight into anticipated mergers that potentially impact Europe's digital market and could require review.

How Grant Thornton can help

At Grant Thornton, we understand the complexities of the DMA and can help your business navigate these new regulations. Our services include:

- **Assurance:** Comprehensive assurance and attestation services for DMA compliance.
- **Compliance assessments:** Evaluate your current operations against DMA requirements.
- **Strategy development:** Create customised compliance strategies to meet DMA standards.
- **Policy drafting:** Develop clear and comprehensive policies for your team.