

CLIENT ALERT

Digital Markets Act: The European Commission Unveils Plans to Regulate Digital 'Gatekeepers'

January 5, 2021

On December 15, 2020, the European Commission (EC) published its [proposal](#) for a Digital Markets Act (DMA). The proposal aims to promote **fair and contestable markets** in the digital sector. If adopted, it could require substantial changes to the business models of large digital platform service providers by imposing new obligations and prohibiting existing market practices. These changes not only would create significant new obligations on “gatekeeper” platforms, but also opportunities for competitor digital service providers and adjacent firms. Further, the proposed requirements of the DMA have the potential to transform the way that businesses engage with “gatekeeper” providers – including, for example, companies that sell goods and services, distribute apps, and/or purchase advertising on large platforms.

Digital Markets Act Proposal: Main Takeaways

- Proposes new rules intended to promote **fair and contestable markets** in the digital sector, which would apply only to providers of “core platform services” designated as “gatekeepers”.
- Defines “**core platform services**” to include online search engines, online marketplaces, social networks, messaging and chat apps, video-sharing platforms, operating systems, cloud computing services, and advertising networks and exchanges.
- Defines “**Gatekeepers**” as providers of core platform services which have a significant impact on the EU internal market, serve as an important gateway for business users to reach customers, and have an entrenched and durable position.
- Provides **quantitative thresholds** based on turnover or market value, and user reach, as a basis to identify presumed gatekeepers. Also empowers the Commission to designate companies as gatekeepers following a market investigation.
- **Prohibits** gatekeepers from engaging in a number of **practices deemed unfair**, such as combining personal data across platforms, ‘wide’ MFN clauses, misusing non-public data about the activities of business users and their customers to gain a competitive advantage, blocking users from uninstalling pre-installed applications, self-preferencing in ranking, etc.
- Imposes certain **affirmative obligations** on gatekeepers, including measures to promote interoperability, data access, data portability, and transparency regarding advertising services.
- Requires gatekeepers to **notify below-threshold mergers** and to accept independent **audits of profiling practices**.
- Puts the Commission in charge of enforcement with extensive investigative powers, including the power to require access to databases and algorithms, and the ability to impose **finances of up to 10% of the gatekeeper’s worldwide annual turnover**.
- Empowers the Commission to impose **structural remedies**, potentially including the divestiture of businesses, for recurring non-compliance.
- Authorizes the Commission to carry out **market investigations** to assess whether new gatekeeper practices and services need to be regulated.

Who Will Be Regulated?

With the DMA, the EC proposes to complement the existing competition rules with **ex ante regulation** of providers of so-called “**core platform services**” that are deemed to have a “**gatekeeper**” position.

Core platform services include online intermediation services (*e.g.* online marketplaces, booking sites, etc.); search engines; social networking services; video-sharing platforms; number-independent interpersonal communication services (*e.g.* messaging and chat apps); operating systems; cloud computing services; and advertising services, including any advertising networks, advertising exchanges and any other advertising intermediation services, provided by a provider of any of the aforementioned other core platform services.

A provider of core platform services is deemed a **gatekeeper** if it fulfills three cumulative conditions:

- It has a **significant impact on the internal market**: this is presumed to be the case if the company achieved an annual turnover in the European Economic Area (EEA) equal to or above € 6.5 billion in each of the last three financial years, or where its average market capitalization or equivalent fair market value amounted to at least € 65 billion in the last financial year, and it provides a core platform service in at least three Member States; and
- It operates a core platform service that serves as an **important gateway for business users to reach their customers**: this is presumed to be the case if the company provides a core platform service that has more than 45 million monthly active end users established or located in the EU (corresponding to roughly 10% of the population of the EU-27) and more than 10,000 yearly active business users established in the EU in the last financial year; and
- It enjoys, or will foreseeably enjoy, an **entrenched and durable position**: this is presumed to be the case if the thresholds in the previous point were met in each of the last three financial years.

A provider of core platform services meeting the above-mentioned thresholds should notify the EC thereof within three months after those thresholds are satisfied. The EC shall then designate the provider as a gatekeeper within 60 days. However, the **presumptions** created by meeting the thresholds are **rebuttable** and the provider can, with its notification, present substantiated arguments to demonstrate that, in the circumstances in which the relevant core platform service operates and considering factors such as entry barriers, it does not qualify as a gatekeeper.

Conversely, even if a company does not meet the quantitative thresholds (or presents substantiated arguments to demonstrate that it does not qualify as a gatekeeper), the EC may still decide to designate it as gatekeeper on the basis of a **qualitative assessment**, taking into account factors such as entry barriers, data-driven advantages, economies of scale and scope, user lock-in effects, etc.

The proposal empowers the EC to adopt **delegated acts** to specify the methodology to determine whether the quantitative thresholds are met as well as to adjust those thresholds to market and technological developments where necessary. The EC shall also **review the gatekeeper designations** on a regular basis and at least every two years.

Do's and Don'ts for Gatekeepers

Providers of core platform services designated as gatekeepers must comply with specific obligations, including both **affirmative obligations ("do's")** and **prohibitions ("don'ts")**. The impact of these obligations can hardly be overstated. Indeed, if adopted as proposed, these obligations would require at least some of the large digital platforms to fundamentally overhaul their business practices and possibly, in some cases, entire business models.

Don'ts	Do's
<ul style="list-style-type: none"> • Combine personal data sourced from their core platform services with personal data from any other services offered by the gatekeeper or third parties, and from signing in end users to other services of the gatekeeper in order to combine personal data, unless the end user has 	<ul style="list-style-type: none"> • Provide advertisers and publishers to which the gatekeeper supplies advertising services with transparent information on prices and/or remuneration with respect to each of the relevant advertising services provided by the gatekeeper;

been presented with a **choice** and provided **consent** as defined by the EU General Data Protection Regulation (GDPR);

- Prevent business users from offering the same products or services to end users through third party online intermediation services at prices or conditions that are different from those offered through the gatekeeper’s intermediation services (*i.e.*, an effective ban on **‘wide’ most favored nation (MFN) or ‘parity’ clauses** in the terms of use of online intermediation services (such as *e.g.* hotel booking sites);
- Restrict the **freedom of business users to choose the promotion and distribution channels** they deem most appropriate to reach end users acquired through the core platform services of the gatekeeper, or restrict the **freedom of end users to acquire content, subscriptions, features or other items outside the core platform services** of the gatekeeper;
- Require business users to include **identification services** provided by the gatekeeper itself as part of the provision of services offered to end users via the gatekeeper’s core platform services;
- Require business users or end users to **subscribe to or register with any other core platform services as a condition of access** to any of the gatekeeper’s core platform services;
- Use any **not publicly available data** about the activities of business users or their end users on the gatekeeper’s platform **to compete with those business users** (*e.g.* where the owner of an online marketplace who is also a trader on that marketplace uses the data it collects about the activities of other traders on the platform purportedly to gain an unfair competitive advantage);
- Prevent end users from **un-installing any pre-**

- Provide advertisers and publishers, upon their request and free of charge, with access to the **advertising performance measuring tools** of the gatekeeper and to the information necessary to carry out their own **independent verification** of the provision of the relevant advertising services;
- Give business users and providers of ancillary services access to and **interoperability** with the same operating system, hardware or software features that are available or used by the gatekeeper itself (*e.g.* access to the APIs used by the gatekeeper’s own applications);
- Ensure effective **data portability** for business users and end users;
- Provide business users free of charge with **effective, high-quality, continuous and real-time access to and use of aggregated and non-aggregated data**, that is provided for or generated in the context of the use of the relevant core platform services by those business users and the end users engaging with the products and services provided by those business users (subject only to the requirements of the GDPR as regards personal data);
- Provide third-party providers of search engines, upon their request, with **access on fair, reasonable and non-discriminatory (FRAND) terms to ranking, query, click and view data** generated by end users of the gatekeeper’s search engines (subject to anonymization of any data that constitutes personal data);
- Apply **FRAND conditions for access** for business users **to the application store** of the gatekeeper.

<p>installed software applications (except if they are essential for the operation of the operating system or device) or from installing and effectively using third-party software applications or software application stores on operating systems of the gatekeeper (<i>i.e.</i>, gatekeepers have to allow so-called “sideloading” of apps and app stores);</p> <ul style="list-style-type: none"> • Rank the own products of the gatekeeper more favorably than similar third-party products; • Technically restrict the ability of end users to switch between and subscribe to different software applications and services to be accessed using the gatekeeper’s operating system. 	
---	--

Core platform service providers will have to comply with these obligations **within six months** of being designated as a “gatekeeper”, although the DMA proposal leaves open a possibility for the **suspension** of, or **exemption** from, specific obligations under certain (very restrictive) conditions.

In addition, gatekeepers are required to **notify the EC of any intended acquisition or concentration** involving another provider of a core platform service or of any other digital sector services irrespective of whether it is notifiable under the EU Merger Regulation or under national merger rules. However, such notification does not constitute a bar to closing the transaction.

Furthermore, within six months of being designated as such, gatekeepers must submit to the EC an **independently audited description of the consumer profiling techniques** they use and update this description on an annual basis.

Market Investigation Mechanism

The DMA proposal empowers the EC to conduct market investigations for three purposes:

- **Identifying gatekeepers that are not captured by the quantitative thresholds** of the DMA as well as assessing the qualification of presumed gatekeepers that have presented substantiated arguments to rebut the presumption;
- **Identifying other services** that should be added to the list of core platform services **or new practices** that may limit the contestability of core platform services or may be unfair and which are not effectively addressed by the existing obligations;
- Identifying proportionate **behavioral or structural remedies** in case of systematic infringement of the rules by a gatekeeper.

Notably, the DMA proposal empowers the EC to **adopt “delegated acts” to “update” the list of do’s and don’ts** where, based on a market investigation, it has identified the need for new obligations addressing practices that limit the contestability of markets or are otherwise unfair. This would mean that the EC could amend the obligations applicable to digital gatekeepers without having to go through the ordinary legislative process, effectively bypassing the EU legislature (the Parliament and the Council).

Enforcement

According to the proposal, the EC will be in charge of enforcing the DMA. To that end, the EC would have **extensive investigative powers** similar to those it has in antitrust investigations, including the power to require information, conduct interviews and conduct on-site inspections (“dawn raids”). Notably, the EC would have the power to **access databases and algorithms** and to require explanations and information about their operational details.

The proposal empowers the EC to adopt decisions ordering gatekeepers to **cease and desist** from non-compliant conduct and to **declare binding commitments** offered by the gatekeepers. Furthermore, **in case of systematic non-compliance**, the Commission can impose any **behavioral or structural remedies** that are proportionate to the infringement committed and necessary to ensure compliance.

The EC would also be able to impose **finest of up to 10% of the company’s total worldwide annual turnover** in the preceding financial year in case of non-compliance with the do’s and don’ts and of up to 1% of total annual turnover for obstructing investigations or failing to submit to audits. The Commission can also impose **periodic penalty payments of up to 5% of average daily turnover** in the preceding financial year per day to enforce compliance with its decisions.

The involvement of national authorities is limited to a “comitology procedure” requiring the EC to consult a **Digital Markets Advisory Committee**, composed of representatives of the Member States, before adopting non-compliance decisions, imposing behavioral or structural remedies, or adopting delegated acts.

As a regulation, the DMA will be directly applicable in the Member States. **Private enforcement** through **national courts** will therefore also be possible.

Relationship with Other Regulation

According to the EC, the DMA proposal complements, and is fully coherent with, the existing Platform-to-business (P2B) Regulation, existing EU and national competition laws, data protection laws (in particular the GDPR) and sector-specific regulation such as the rules applicable to electronic communications services (in particular the European Electronic Communications Code (EECC), which the Member States had to transpose into national law by 21 December 2020).

Unlike the **P2B Regulation**, which applies (since 12 July 2020) to all online intermediation services and search engines in their relationships with business users, the DMA is a deliberately asymmetric regulatory instrument, *i.e.* one which applies only to a subset of very large platforms. However, the DMA applies in respect of a wider range of platform services and in the gatekeepers’ relationships with both business users and consumers. Whereas the P2B Regulation only imposes relatively light-touch obligations of fairness, transparency and effective redress, the DMA includes much more far-reaching and specific rules.

The DMA proposal purports to complement **existing competition laws** by addressing unfair practices that either fall outside the scope of those laws or cannot be as effectively addressed by them, considering that antitrust enforcement only intervenes *ex post*, on a case-by-case basis, and usually only after a lengthy investigation. According to the Commission, the DMA proposal, with its list of do's and don'ts, is based on its own antitrust enforcement experience as well as on the findings of several expert reports on the application of competition law in digital markets. If the DMA is adopted as proposed, the practices that it blacklists will be prohibited *ex ante* if applied by designated gatekeepers, without the need to show that they infringe EU or national antitrust laws.

The DMA proposal also purports to complement existing **data protection laws** by, inter alia, imposing transparency obligations for “deep” consumer profiling and a mandatory opt-out requirement for combining data across core platform services. At the same time, the data access and portability requirements provided for in the proposal are specifically subject to the requirements of the GDPR when applied to personal data.

Next Steps

The DMA proposal and the parallel proposal for a Digital Services Act are subject to the ordinary EU legislative procedure. That means that they will go through a lengthy negotiation process between the European Parliament and the Council, which is expected to last at least 1.5 years and likely will entail numerous amendments to the texts before a compromise between the two co-legislators is reached. Once adopted, the Act is expected to enter into force six months after its publication and will be directly applicable across the EU.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Thomas De Meese

Partner – Brussels

Phone: +32.2.282.1842

Email: tdemeese@crowell.com

Jeane A. Thomas, CIPP/E

Partner – Brussels, Washington, D.C.

Phone: +32.2.282.4082, +1.202.624.2877

Email: jthomas@crowell.com

Karl Stas

Senior Counsel – Brussels

Phone: +32.2.214.2888

Email: kstas@crowell.com