Global AppCon'22
Competition and Privacy
ACT | The App Association

Digital Markets Act (DMA)

The DMA is a new European Union (EU) law that aims to limit the market power of large online platforms. The DMA allows the European Commission (EC) to designate large online platforms as "gatekeepers" if they meet certain quantitative thresholds, and then subjects them to obligations and prescribes things they can and cannot do.

By creating new obligations for "gatekeeping" platforms, the DMA will have far-reaching consequences for the companies that operate on them, including small app developers and tech small and medium-sized enterprises (SMEs). Some obligations may enable fairer and more competitive digital markets in the short term, but others could generate much greater risks for the app ecosystem in the long run. Some of the negative consequences include:

1.

Lower security and trust in the app ecosystem:

The DMA's broad obligations for gatekeepers to allow sideloading and enable interoperability could unintentionally open the gate to malicious actors and put end-users' data and safety at risk. Our members rely on the safe environment that platforms provide to keep bad actors out of the app ecosystem, gain consumer trust, and innovate. These provisions may unintentionally hurt them by making the app ecosystem less secure and decreasing consumer trust.

2.

Level the playing field for the large app developers only:

Reducing security and trust in the app ecosystem will only level the playing field for gatekeepers and large developers, while further widening the gap between large and small actors. Small developers who rely on the platforms to gain consumer trust and who do not have the resources to compete with the big brands will suffer.

3.

Risk locking small app developers out of the market:

Obligations for gatekeepers that mandate the use of "choice screens," lists of only the main and largest service providers for default apps that consumers can then choose from, could lock small app developers out of the market as they are unlikely to be included in the list of choice screen options.

Who falls in the scope of the DMA?

The European Commission can only designate undertakings that provide a core platform service (CPS) and that meet three quantitative thresholds as a gatekeeper under the DMA.

Core platform services – Art. 2(2)

- online intermediation services, including
- marketplaces and app stores
- search engines
- social networks
- video-sharing platforms
- operating systems
- cloud services
- number independent interpersonal communications
- online advertising networks
- web browsers
- virtual assistants

Quantitative thresholds - Art. 3(2)

€7.5 billion+

in turnover in the European Economic Area (EEA, which comprises the EU plus Iceland, Liechtenstein, and Norway)

€80 billion+

of market capitalization

45 million

monthly users and 10,000+ business users in the last financial year.

SMEs are specifically excluded from gatekeeper status although the EC may place some obligations on what it considers as "emerging gatekeepers." If a company providing a CPS has a significant impact on the internal market and enjoys an entrenched and durable position or it is foreseeable that it will do so in the near future, it can be designated as an emerging gatekeeper, even if it does not meet the quantitative thresholds.

Obligations for designated gatekeepers

Once the Commission designates a company as a gatekeeper, it needs to comply with the DMA's list of requirements included in Articles 5, 6, and 7. These obligations apply immediately after a company's gatekeeper designation. The Commission can further specify the obligations in Articles 6 and 7 through a regulatory dialogue with the gatekeeper.

The most concerning provisions for app developers include:

Obligation to allow the uninstallation of apps and change of default settings - Art. 6(3)

A gatekeeper is to technically enable end-users to uninstall any software applications on its operating system (OS) unless the apps are considered essential for the functioning of the OS or the device and cannot technically be offered on a stand-alone basis by third parties.

Additionally, a gatekeeper needs to ensure users see a prompt to switch default apps for online search engines, virtual assistants, or web browsers, and go through **a list of the main third-party services available**.

What does this mean for app developers?

Choice screens present an artificial choice to consumers, giving them the impression that only a limited number of apps are available for a certain service when, in fact, there may be dozens or hundreds of alternatives. The only developers that will benefit from this obligation are those large enough to be an option on the list of choice screens. This obligation puts smaller developers at risk of being locked out of the market entirely

Mandated sideloading - Art. 6(4)

A gatekeeper is to technically enable the installation and effective use of third-party software apps or app stores on end-users' devices. Additionally, gatekeepers cannot prevent sideloaded apps or app stores from prompting end-users to set those apps or app stores as their defaults. A gatekeeper can take measures to ensure that sideloaded apps and app stores do not endanger the integrity of the hardware or OS provided by the gatekeeper, only to the extent strictly necessary and proportionate.

What does this mean for app developers?

Consumers are willing to trust apps they download from app stores because of years of positive experiences with the extra scrutiny and safeguards app stores offer to ensure safe and well-functioning apps. This provision would force mobile platform operators to allow unvetted sideloaded software— which could include malware, spyware, and other apps that only exist to harm consumers—onto consumer devices by default.

Mandated Interoperability with hardware and software features - Art. 6(7)

A gatekeeper must **provide suppliers of services and of hardware with free and effective interoperability with the same hardware and software features accessed or controlled via the OS or virtual assistant of the gatekeeper.** Additionally, business users and alternative providers of services offered with or in support of a CPS should be allowed free and effective interoperability with the same OS, hardware, or software features as the gatekeepers', regardless of whether those features are part of the operating system. Limited safeguards include that a gatekeeper can take measures that are strictly necessary and proportionate to ensure that interoperability does not compromise the integrity of its OS, virtual assistant, hardware, or software features.

What does this mean for app developers?

Providing full access to all the core features on a device to business users and providers of services and hardware could allow malicious third parties to reach sensitive device features and circumvent protections. For example, such actors could access cameras, contact lists, or virtual private networks without end-user permission, or track other devices in the same facility and hijack the functionality of other apps, putting end-users' security and privacy at serious risk.

Interoperability obligation for number-independent interpersonal communication services (NICS) – Art. 7

A gatekeeper providing a NICS must make basic functionalities of service interoperable with the NICS services of other providers by providing the necessary technical interfaces that facilitate interoperability, upon request, and free of charge.

Interoperability obligations applicable immediately concern end-to-end text messaging and sharing of images, voice messages, videos, and other attached files between two individuals. Within two years, obligations are extended to group texts and sharing of the same files, and within four years, to voice and video calls between two users or a user and a group chat.

What does this mean for app developers?

Interoperability between messenger services raises several concerns regarding data security, encryption, and data minimization. For example, limiting data collection and data sharing is one of the key features that providers of messenger services use to differentiate themselves from gatekeepers' services. Additionally, interoperability generally requires mirror features and common interfaces and protocols to achieve full inter-connection, and this provision will lead to a degree of product homogenization, limiting innovation in this field.

Who falls in the scope of the DMA?

The European Commission can only designate undertakings that provide a core platform service (CPS) and that meet three quantitative thresholds as a gatekeeper under the DMA.

Third parties, including SMEs, can provide comments on the Commission's preliminary findings in the framework of this dialogue.

Suspension of obligations for gatekeepers

The European Commission can suspend in whole or in part a specific obligation of a gatekeeper and consider the impact of the obligation on the economic viability of the gatekeeper as well as third parties, in particular SMEs (Art. 9).

Market investigations to define new core platform services and obligations

The European Commission can conduct market investigations to examine whether to update the list of CPS or the list of obligations (Art. 19). Where appropriate, it can propose to amend the DMA to remove existing services from the list of core platform services or to remove existing obligations from Articles 5, 6, or 7.

The Commission may consult third parties such as app developers who are subject to practices under investigation.

What's next?

The DMA still needs to be formally approved by the Council of the European Union and the European Parliament. Once this process done, it is expected to enter into force as early as October 2022, and gatekeepers to be fully compliant with the DMA obligations by the beginning of 2024.

The DMA is a complex piece of legislation, and the practical implementation of this new law is critical to ensure it benefits all businesses and does not harm small businesses. We will keep our members informed on all the developments as regards to its implementation, enforcement, and review.

ACT | The App Association

1401 K Street NW Suite 501
Washington, DC 20005

202.331.2130 @ACTonline
ACTonline.org/ actonline.org