DIGITALEUROPE

2 FEBUARY 2022

Final steps towards a targeted and predictable Digital Markets Act

Executive summary

DIGITALEUROPE welcomes the EU's efforts to create more contestable digital markets. As the European institutions enter the final stages of negotiations on the proposed Digital Markets Act (DMA),[1] the focus should be on achieving a proportionate and workable framework.

Key to this end are a precise scope and predictable obligations, which should be restricted to those proved necessary to facilitate contestability and fairness. In particular:

- Co-legislators should maintain the initially proposed scope. Any expansion of scope (to smart TVs, browsers and voice assistants) or obligations (access to operating systems beyond ancillary services, access to new core platforms services, full-service interoperability or changes to defaults) is not yet supported by adequate evidence of market failure and ignores potential impacts on the market and consumers.
- The strengthened regulatory dialogue proposed by the co-legislators should be further improved to allow the DMA provisions to be as targeted as possible and create the discretion to agree on a longer compliance timeline if necessary.
- We welcome the safeguards linked to interoperability, technical access and anti-steering, as offered by the European Parliament. They will be key to ensuring that the DMA is in line with other key public policy objectives, including cybersecurity and data protection.

[1] COM/2020/842 final.

DIGITALEUROPE
Rue de la Science, 14A, B-1040 Brussels
T.+32 (0) 2 609 53 10 / www.digitaleurope.org / @DIGITALEUROPE
EU Transparency Register: 64270747023-20

Table of contents

- Executive summary 1
- Table of contents 2
- Scope and designation of gatekeepers 3

Core platform services 3

Designation criteria 3

- Obligations 4

Combining personal data 4

Data access and portability 5

Pre-installed apps 5

Fair and non-discriminatory ranking 5

Anti-steering 6

Access and interoperability 6

Scope and proportionality 6

Safeguards 7

Interoperability of communications services and social media 7

Tying/bundling 7

Fair and non-discriminatory access conditions for CPSs 8

- Sanctions and remedies 8
- Regulatory dialogue 8
- Implementation timeline 9

Scope and designation of gatekeepers

Core platform services

The core platform services (CPSs) captured by the proposal are very different in nature and business model. Some are interactional (social networking, video sharing and communications services) or transactional (intermediaries and search engines), while others are technical platforms (operating systems). Finally, 'cloud services' is a generic term covering a plethora of different services.

Clarifying the DMA's scope is therefore indispensable, particularly considering that all these companies will potentially be subject to the same obligations.

The CPS list should be backed by strong evidence of contestability issues and accompanied by an impact assessment. For this reason, we do not support the Parliament's attempts to expand the scope further with the proposed inclusion of connected TVs, internet browsers and voice assistants in the list of CPSs and reference to connected cars in the recitals. There is no clear evidence base for their inclusion. Some of these services, in fact, exhibit very low entry barriers, fierce competition or significant multi-homing by users. The expansion also raises further questions about how the thresholds would apply to these services and the obligations operationalised.

Virtual assistants should not be regulated in their own right as they primarily provide an interface to use other services. The definition of operating systems is also too generic and broad. Embedded product-related operating systems are designed with only limited functionality and very specific purpose for a particular type of device. They are not comparable with operating systems on computer hardware systems. We recommend aligning with the definition of operating system included in the European Accessibility Act which will create a more consistent and effective legal framework.[2]

By contrast, we welcome the clarifications introduced by the Council regarding changes to the DMA's scope. Any substantial changes – be they to the covered CPSs, to the obligations or to pertinent definitions or thresholds – should not be carried out via delegated acts but only via the ordinary legislative procedure, as these are essential elements of the framework.

Designation criteria

The three main criteria outlined in Art. 3(1) to designate a gatekeeper are vague, despite being the ultimate tests for intervention. This makes it difficult to assess

[2] Art. 3(38), Directive (EU) 2019/882.

whether a company falls into scope and to ensure proportionate regulatory outcomes.

Importantly, all thresholds point to size, but size alone does not demonstrate a lack of contestability in the market. It is crucial for the designation process to consider a platform's characteristics and existing competitive pressures, such as the degree of multi-homing among users and/or business users. We welcome the many clarifications provided to this effect by the co-legislators in Art. 3(6), notably linked to multi-homing.

However, the criteria overall remain vague or provide limited information in demonstrating market power. In particular:

- Turnover, market capitalisation or user numbers are not in themselves an indicator of significant impact, while relevant criteria like market share are not considered.
- References to 'other market characteristics' or 'other structural business or services' in the Council's position are catch-all and ambiguous.
- Reference to a mere 'ability to implement conglomerate strategies' in the Parliament's is not only difficult to define, but is inherently speculative and makes it prohibitive to demonstrate otherwise.
- The requirement of providing a CPS in at least three EU Member States raises the question of whether companies that otherwise fulfil all other criteria do not pose the same concerns.

Obligations

Combining personal data

Art. 5(a) would force gatekeepers to require consent for combining data, while the General Data Protection Regulation (GDPR) offers other legal bases for processing, including when combining data from different services.[3]

There are justified reasons for combining data. These include security, fraud prevention and customer support, where legitimate interest and contract necessity, among other GDPR legal bases, should remain available.

Online services are targets of cyberattacks and fraud. Data is vital to maintaining the security and integrity of services. An obligation not to combine data would adversely affect companies' ability to protect their services and customers.

[3] Regulation (EU) 2016/679.

Data access and portability

It remains unclear how the data access and data portability obligations, which have largely been left unchanged by the co-legislators, would be implemented in practice.

Data is not technically easy to transfer, particularly continuously and in real time as mandated by Arts 6(1)(h) and (i). There are presently no commonly agreed standards or infrastructure for exporting data. As a result, the provision should not enter into force until standardisation bodies have developed or identified suitable standards and technical specifications.

Pre-installed apps

The uninstallation of preinstalled apps is already embraced by many service providers. However, some pre-installed apps are essential to the functioning of a device and to the adequate out-of-the-box experience that consumers expect. This is outlined correctly in Art. 6 (1)(b).

The Parliament has proposed moving the obligation to allow end-users to uninstall preinstalled apps to Art. 5. Given that what constitutes an app that is 'essential for the functioning of the operating system or of the device' is open to interpretation, this obligation should remain within Art. 6 and thus be subject to further specification.

The Parliament has also proposed an additional requirement for the introduction of mandatory choice screens. Whilst improving consumer choice is an important public policy objective, mandated changes that would damage user experience should be avoided. Alternative apps can easily be found on application stores, offering a fair way for alternative service providers to be discovered by end-users.

Fair and non-discriminatory ranking

Any prohibition of self-preferencing gatekeepers' own services (Art. 6(1)(d)) should be limited to ranking that deliberately demotes business users' offers or boosts the prominence of a gatekeeper's own offering.

The Parliament's proposed expansion of this provision to all CPSs, via changes to the definition of 'ranking,' is concerning. It is unclear what it would mean for services which do not entail classic ranking features, such as cloud, messenger or social networking services. Similarly, the Parliament's additional suggestion to expand the prohibition to 'other settings' is too undetermined to provide sufficient legal certainty.

Anti-steering

The anti-steering provision (Art. 5(c)) runs the risk of turning marketplaces or app stores into what are essentially unpaid advertising platforms, allowing businesses to capture users and direct them to fulfil purchases on their own sites.

This obligation, which would be unacceptable offline, undermines legitimate commission-based business models. Beyond free-riding concerns, the provision is also likely to pose a risk of payment fraud. At the very least, a safeguard should be introduced to allow operators to tackle any abuse of the provision, as proposed by the European Parliament.

Access and interoperability

Access to technology and interoperability requirements must be proportionate and focus on areas that are key to achieving market contestability.

Scope and proportionality

The DMA introduces general interoperability obligations on a select number of companies without considering the need for industry-led standards across the digital economy.

Access and interoperability must focus on technologies crucial to delivering the goals of contestability and fairness. In many cases, access through open application interfaces (APIs) is sufficient; in other, much rarer occasions, full service interoperability may be required.

The DMA should allow specification through regulatory dialogue to design access conditions that are suitable. This may include offering access that delivers competitive equivalence, as opposed to exactly the same access, so as to ensure contestability without putting user safety at risk.

Certain amendments that have been put forward would unduly extend the scope of the DMA's interoperability requirements. Unrestricted full service access appears disproportionate, especially where common standards or interfaces do not exist. Mostly notably:

- The Parliament's broad extension of Art. 6(1)(f) to all services and hardware would allow a virtually limitless scope of access requests from third parties, which would be compounded by the suggestion that access must be provided free of charge.
- The Parliament's introduction of a definition of interoperability in Art. 2(23a) that points to full service interoperability across the board is

disproportionate and presupposes the existence of standards not currently available.

Safeguards

The introduction of safeguards in Arts 6(1)(c) and (f) referring to integrity, security and data protection is welcome. These safeguards will allow gatekeepers to limit user exposure to bad actors, fraud and illegal content through both technical means and the enforcement of platform governance policies. This is particularly relevant given sensitive data generated and stored on devices.

The approach proposed by the Parliament will better tackle end-user protection issues raised by interoperability requirements and limit exposure to problematic software and content at the source. The Council's emphasis in Art. 6(1)(c) on leaving end-users in charge of protecting themselves is insufficient as cybercrime is primarily carried out via social engineering.

Interoperability of communications services and social media

Any introduction of service interoperability requirements, such as those proposed by the Parliament targeting social media platforms and number-independent interpersonal communications services (NI-ICS), must be based on strong evidence of market failure and thorough impact analysis.

For social media services, the Parliament's proposal would lead to a high degree of uncertainty as to the relevant scope and features. Imposing such requirements would require a much deeper assessment of the challenges companies may face in preserving the security and integrity of their services when facing access requests from third parties.

The matter of NI-ICS interoperability is already covered under the European Electronic Communications Code (EECC), which includes a process and test for intervention in this space that the DMA should not preclude.[4]

Tying/bundling

We are concerned by the Parliament's proposed extension of Art. 5(e), which was originally designed for identification services, to all ancillary services. Because the definition of ancillary services is open-ended, this obligation risks being equally indeterminate. Like any other DMA obligation, this requirement

[4] Art. 61, Directive (EU) 2018/1972.

should only target areas where there is evidence of a lack of market contestability.

We suggest limiting the scope of tying and bundling prohibitions to technical actions that serve to prevent switching and seek to deliberately break interoperability.

Fair and non-discriminatory access conditions for CPSs

The Parliament's proposal to extend the fair access conditions obligation (Art. 6(1)(k)), which was originally designed only for app stores, to all CPSs is concerning.

This profoundly changes the nature of the original obligation with no supporting evidence, and it is unclear how such a requirement would apply to the various CPSs.

Sanctions and remedies

The proposed three-strike approach – basing structural remedies on three infringements in a given time period – raises questions as to how the Commission's enforcement priorities may impact the number of infringements, whether investigations can be split into several infringements, and whether infringements need to happen on the same CPS or across all services. In the latter case, it is unclear which structural measure would be applied. The Parliament's further easing of the imposition of structural remedies, as of two infringements in 10 years, appears excessive.

In addition, the Commission's proposal featured the highest possible sanctions outside competition law, at 10 per cent of annual turnover. The Parliament's proposal to double the maximum sanction to 20 per cent and the introduction of a 4 per cent minimum fine appear disproportionate.

Regulatory dialogue

Regulatory dialogue is key to successful DMA implementation – it will create a better understanding of market dynamics, platforms' and users' interests, and technical considerations.

While the Council's clarifications on this point are helpful, they fall short of providing the level of legal certainty necessary for participating companies, such as a comfort letter, which could hold up in potential court proceedings or if the Commission chose to change its view on the implementation of certain provisions. Companies need to be able to rely on the regulatory dialogue and on its outcomes given the DMA's significant operational and technical requirements.

Additionally, we caution against moving obligations from Art. 6 to Art. 5, where they would not be subject to regulatory dialogue. In fact, several of the Art. 5 obligations, such as Arts 5(a) and (c), will in practice require a dialogue with the Commission and should therefore be moved to Art. 6.

Implementation timeline

To be effective, the DMA needs to allow businesses sufficient time for implementation, proportionate to the changes needed.

Several obligations require significant changes to business models, in-depth legal assessment and profound technical implementation work. For example, introducing interoperability of systems may require a complete rebuild of key functions.

In light of this, regulatory dialogue should have the discretion to agree on a longer compliance timeline if necessary. The Council's proposal to add six months before notification deadlines are triggered is welcome, but is still significantly shorter compared to other EU regulations with similarly complex requirements such as the GDPR, which set out a two-year implementation period.

FOR MORE INFORMATION, PLEASE CONTACT:

Hugh Kirk

Senior Manager for Digital Commerce Policy

hugh.kirk@digitaleurope.org / +32 490 11 69 46

Alberto Di Felice

Director for Infrastructure, Privacy and Security Policy

alberto.difelice@digitaleurope.org / +32 471 99 34 25

About DIGITALEUROPE

DIGITALEUROPE represents the digital technology industry in Europe. Our members include some of the world's largest IT, telecoms and consumer electronics companies and national associations from every part of Europe. DIGITALEUROPE wants European businesses and citizens to benefit fully from digital technologies and for Europe to grow, attract and sustain the world's best digital technology companies. DIGITALEUROPE ensures industry participation in the development and implementation of EU policies.

DIGITALEUROPE Membership

Corporate Members

Accenture, Airbus, Amazon, AMD, Apple, Arçelik, Assent, Atos, Autodesk, Bayer, Bidao, Bosch, Bose, Bristol-Myers Squibb, Brother, Canon, Cisco, DATEV, Dell, Eli Lilly and Company, Epson, Ericsson, ESET, EY, Facebook, Fujitsu, GlaxoSmithKline, Global Knowledge, Google, Graphcore, Hewlett Packard Enterprise, Hitachi, HP Inc., HSBC, Huawei, Intel, Johnson & Johnson, Johnson Controls International, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Mastercard, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, Nemetschek, NetApp, Nokia, Nvidia Ltd., Oki, OPPO, Oracle, Palo Alto Networks, Panasonic Europe, Philips, Pioneer, Qualcomm, Red Hat, ResMed, Ricoh, Roche, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Siemens Healthineers, Sky CP, Sony, Sopra Steria, Swatch Group, Technicolor, Texas Instruments, TikTok, Toshiba, TP Vision, UnitedHealth Group, Visa, Vivo, VMware, Waymo, Workday, Xerox, Xiaomi, Zoom.

National Trade Associations

Austria: IOÖ
Belgium: AGORIA
Croatia: Croatian Chamber of Economy
Cyprus: CITEA
Denmark: DI Digital, IT BRANCHEN, Dansk Erhverv
Estonia: ITL
Finland: TIF
France: AFNUM, SECIMAVI, numeum
Germany: bitkom, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: Technology Ireland
Italy: Anitec-Assinform
Lithuania: Infobalt
Luxembourg: APSI
Moldova: ATIC
Netherlands: NLdigital, FIAR
Norway: Abelia
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS
Slovakia: ITAS
Slovenia: ICT Association of Slovenia at CCIS
Spain: AMETIC
Sweden: TechSverige, Teknikföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
United Kingdom: techUK