

**C L I F F O R D**  
**C H A N C E**



**THE EU'S  
PROPOSALS FOR  
FAR-REACHING  
REGULATION  
OF THE DIGITAL  
SECTOR**



**— THOUGHT LEADERSHIP**

**DECEMBER 2020**



### Key issues

- Which digital sector players would be caught by the proposed regime?
- What do the two pieces of legislation seek to achieve, and how do they differ?
- What new obligations would be imposed on digital platforms and other intermediaries?
- How will the regimes be enforced?
- When are they likely to come into force, and how much are they likely to change before then?



Europe is again out front in the world and taking dramatic action on the tech regulation front - far beyond what any other country or region is contemplating or pursuing.



— **DIETER PAEMEN**  
Partner, Brussels

## THE EU'S PROPOSALS FOR FAR-REACHING REGULATION OF THE DIGITAL SECTOR

The European Commission (**Commission**) has announced far-reaching proposals for regulation of digital platforms and online intermediaries. The Digital Markets Act (**DMA**) will impose on digital platforms that are designated as “gatekeepers” a long list of obligations to refrain from practices that are considered to limit competition or to otherwise be unfair. In contrast, the Digital Services Act (**DSA**) focuses on regulating the way that providers of online intermediary services interact with their customers and users, and their obligations in respect of harmful or illegal content, in order to create “uniform rules for a safe predictable and trusted online environment”.

In combination, the two pieces of proposed legislation will create Europe's most dramatic and interventionist sector-specific regulatory regime in decades, and would require significant changes to the business practices of digital sector players such as Google, Facebook and Apple, but also potentially smaller competitors.

While it is likely to be around two years or more before these proposals result in binding obligations, they are unlikely, in our view, to be significantly watered down during the legislative process.

### THE DIGITAL MARKETS ACT

The Commission has concluded that certain digital platforms should be subject to ex-ante regulation because, in its view:

- a small number of “gatekeeper” platforms have come to dominate the digital economy, by intermediating a large portion of the access between consumers and businesses, be it for information, services, or goods;
- ex-post antitrust enforcement has not been entirely effective in addressing the conduct of these companies, in particular because of the time it takes and the difficulties of devising genuinely effective remedies; and
- current EU competition law is not structured in a way that allows certain issues raised by the digital economy to be addressed. For example, existing law provides no means of preventing markets with a large but not yet dominant player from irreversibly tipping in favour of that company.

### What activities does the DMA capture?

The DMA is not intended to apply horizontally to the entire digital sector, but only to so-called Core Platform Services (**CPS**). These are: (i) online intermediation services (e.g., marketplaces, app stores); (ii) online search engines (e.g., Google); (iii) online social networking services (e.g., Facebook); (iv) video sharing platform services (e.g., YouTube); (v) number-independent interpersonal electronic communication services (e.g., messaging services like WhatsApp, Facetime, videoconferencing apps, email services); (vi) operating systems; (vii) cloud services; and (viii) advertising services (provided by a provider of any of the core platform services listed above).

### Which companies are subject to the DMA?

Not all companies active in core platform services would be subject to the DMA – only so-called “gatekeepers” that meet three criteria:

- A size that impacts the EU internal market: this would be presumed if the company achieved an annual EEA turnover of €6.5 billion or more in the last three financial years, or where its average market capitalisation 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.
- The control of an important gateway for business users towards final consumers: this would be presumed if the company operates a core platform service with more than 45 million monthly active EU end users (roughly 10% of the EU's population) and more than 10,000 annual active EU business users in the last financial year;
- An (expected) entrenched and durable position: this would be presumed if the criteria in the bullet point above are met in each of the last three financial years.

Platforms that meet the quantitative metrics would only be able to avoid categorisation as a gatekeeper if they demonstrate to the Commission that the three criteria above are not met (despite the quantitative thresholds being satisfied), with reference to factors such as numbers of users, the position of the provider, absence of entry barriers deriving from network effects and data-driven advantages, the degree of user “lock in”, and structural market characteristics. Similarly, platforms that do not meet the quantitative criteria could be designated by the Commission as gatekeepers on the basis of a qualitative assessment of those same factors, carried out in the context of a “market investigation” procedure with a non-binding 12 month timetable. This is intended to allow the Commission to designate as gatekeepers platforms that do not yet have an “entrenched and durable position” but can be expected to obtain one in the future. These “emerging gatekeepers” would be subject to a more limited set of obligations than other gatekeepers.

Market investigations could also be used to identify whether other digital sector services or practices should be brought within the scope of the Regulation (a 12 month process) and to design additional

remedies for gatekeepers that systematically infringe their obligations under the DMA (a 24 month process). Systematic infringers could be subject to both behavioural and structural remedies, meaning that the Commission would have powers to break up large platform operators in certain circumstances.

These possibilities for “market investigations” are the last remnants of a much wider and non-sector specific regime that the Commission had proposed earlier this year (under the name “New Competition Tool”), but has now abandoned.

## Obligations and prohibitions

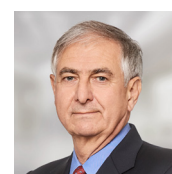
The DMA would create a long list of obligations for gatekeepers to refrain from practices that limit contestability of markets or are otherwise unfair. Some would apply without any possibility for further specification or clarification by the Commission, while others would allow for the Commission to further specify what individual gatekeepers must do in order to comply with them.

Obligations that are not subject to further specification are as follows. To:

- refrain from combining personal data from core platform services with personal data from other services;
- refrain from restricting business users’ freedom to freely price products on other platforms, e.g., through “most-favoured nation” clauses;
- allow businesses on the platform to promote and contract with users outside the platform, and, where such off-platform purchases take place, to allow those businesses to provide those products and services through their own software applications;
- refrain from restricting business users from complaining to public authorities;
- refrain from requiring business users to use, offer or interoperate with an identification service of the gatekeeper;
- refrain from making access to any core platform services conditional on users registering or subscribing to any other core platform services;



**Even if it has powers to do so, the EU is unlikely to risk its relationship with the US by threatening to break up American icons, and the Biden administration is not going to let that happen easily.**



—**THOMAS VINJE**  
Partner, Co-Chair, Global Antitrust Group, Brussels



**The DMA would impose a multitude of far-reaching ex-ante obligations on large digital platforms to enable interoperability with their products and thereby could facilitate competition from smaller players.**



—**MICHAEL DIETRICH**  
Partner, Düsseldorf



**As is the case under the competition rules, binding information requests could be addressed to third parties, so even parties that are not caught by the legislation would be likely to face increased administrative burdens when it enters into force.**



**— IWONA TERLECKA**  
Counsel, Warsaw

- provide advertisers and publishers to which a platform supplies advertising services with certain information about pricing of those services;
- inform the Commission about intended acquisitions of any other digital services before closing their transactions, irrespective of whether the merger control thresholds for EU or national filings are met. This obligation will give the Commission new scope to monitor and control gatekeepers' M&A, when combined with its new policy of accepting EU Merger Regulation jurisdiction over small mergers that are not otherwise notifiable anywhere; and
- submit to the Commission an independently audited annual report describing any techniques applied by the gatekeeper for profiling of consumers across its core platform services.

Certain other obligations would apply automatically, but could be further specified by the Commission if it concluded that a gatekeeper's compliance measures were ineffective. In order to obtain clarity on the scope of these obligations, gatekeepers would be able to ask the Commission to carry out a review of its actual or proposed compliance measures. Obligations that could be subject to such further specification are as follows. Obligations to:

- refrain from using non-public data from its business users to provide services in competition with these users;
- allow uninstallation of preinstalled applications unless technically essential;
- allow installation of third-party apps and app stores on its operating systems, to the extent these do not endanger the integrity of hardware or operating systems provided by the gatekeeper;
- refrain from preferencing own services and products versus those of third parties in rankings;
- refrain from technical restrictions on users switching between (or subscribing to) different software applications and services that are

accessed using the gatekeeper's operating system;

- provide competing third-party providers of ancillary services non-discriminatory access to interoperability and features of their operating system, hardware or software;
- provide advertisers and publishers with access to the performance measuring tools and information that allows them to carry out their own independent verification of ad inventories;
- facilitate data portability;
- provide business users with access to data generated by their use, and their users' use, of the gatekeeper's core platform services;
- provide third party providers of online search engines with fair, reasonable and non-discriminatory access to ranking, query, click and view data generated by users of the gatekeeper's online search engine; and
- apply fair and non-discriminatory general conditions of access for business users to its app store.

The DMA provides for procedures whereby gatekeepers could obtain exemptions from most of the above obligations on public interest grounds (public morality, public health or public security). Obligations could also be suspended by the Commission if a gatekeeper shows that their application will endanger its economic viability, due to exceptional circumstances beyond its control.

## **Enforcement and compliance**

Enforcement would be by the Commission alone (unlike the DSA there is no role for national authorities), although as a directly-applicable Regulation, the legislation would give parties that are harmed by an infringement of the DMA the right to claim damages in national courts. The Commission will have broadly the same investigative and enforcement powers as under the competition rules, including powers to gather information, to carry out dawn raids, to accept commitments and



to impose remedies and fines of up to 10% of group worldwide turnover. Infringement decisions would be appealable to the EU Courts.

## THE DIGITAL SERVICES ACT

While the DMA focuses on the competitive conduct of digital intermediaries, the DSA will regulate the way that they interact with their customers, and their obligations in respect of harmful or illegal content, in order to create “uniform rules for a safe predictable and trusted online environment”.

### New obligations for digital intermediaries

Under the DSA, there will be four layers of obligations (various exceptions apply for micro and small enterprises).

The first layer applies to all providers of digital services that connect EU consumers to goods, services, or content (intermediary services). That includes providers located or established outside the EU that have a significant number of EU users, or which target activities towards one or more EU member states.

All providers of intermediary services would be required to have an EU point of contact or (if they do not have an establishment in the EU) a legal representative in the EU for communications with regulators, including the new “Digital Services Coordinators” (DSCs) that each EU member state will be required to designate as their primary national enforcer of the DSA. Providers would also have obligations to provide clear information in their terms and conditions on any service restrictions that apply to their customers’ content, including information on content moderation tools and policies, and would have to publish detailed reports at least once a year regarding their content moderation activities.

The second layer applies to a specific type of intermediary service provider: hosting services providers, which store information provided by their customers (e.g., cloud storage providers, online platforms). These would have additional

obligations to implement mechanisms to allow third parties to notify them of illegal content and to act on such notifications in a timely, diligent and objective way, with priority accorded to notifications made by “trusted flaggers” that are designated by national authorities. When restricting access to a customer’s content, hosting services providers would have to provide the customer with a statement of reasons containing certain information to help customers understand the reasons for the decision and how it was made.

The third layer applies specifically to online platforms, a subset of hosting service providers which disseminate their customers’ information to the public, e.g., an online booking or reservation platform. Online platforms would be required to give customers access to mechanisms to resolve disputes relating to decisions to restrict access to their information or to suspend or terminate their service or account, including a user friendly complaints system and out-of-court dispute settlement. They would also have obligations to suspend their services to customers that frequently provide manifestly illegal content and to alert law enforcement or judicial authorities promptly if they become aware of any information giving rise to a suspicion of a serious criminal offence involving a threat to the life or safety of any person. Additional reporting requirements would include information on suspensions imposed, out-of-court dispute settlements, the use of automatic content moderation tools and numbers of average active monthly users.

Business to consumer (B2C) platforms would be required to take certain steps to verify the identity and traceability of traders that use their platforms, and online platforms that display advertising would have to ensure that users can tell that what they are being shown is an advert.

The fourth and final layer applies to “very large online platforms”, which are defined as online platforms with 45 million or more average monthly active users in the EU. In addition to all the other obligations described above, very large online platforms would be required to:



**The Digital Services Act brings a much-needed update to the regulatory regime brought in by the 2000 e-commerce directive. The innovative services that have emerged in the last 20 years have transformed the daily lives of citizens, but they have also brought new risks and challenges for society**



—**DESSLAVA SAVOVA**  
Partner, Paris



The proposals would mean the end of Europe's fragmented approach to tech regulation, as the new Regulations would apply directly in the member states, becoming the new "civil code" for digital services intermediaries and e-platforms.



—**JOACHIM FLEURY**  
Global Head of TMT, London

- assess and mitigate systemic risks, such as dissemination of illegal content, negative effects on the exercise of fundamental rights and intentional manipulation of their services;
- submit to external independent audits at least once a year;
- appointment at least one compliance officer to monitor compliance with the DSA and provide compliance data to DSCs and the Commission; and
- provide more frequent reports than other online platforms, containing additional information on risk assessments carried out, risk mitigation measures implemented and the results of audits.

Very large online platforms that make automated recommendations to users (e.g., as a result of a user's search) would also have to provide in their terms and conditions information on the main parameters used in their "recommender systems" and any options for users to modify or influence those parameters. Those that display advertising would be required to publish (through application programming interfaces) a repository containing specific information about the adverts that they have displayed.

### Continued exemption from liability for digital intermediaries

As a corollary to the various obligations imposed, digital intermediaries would continue to enjoy the legislative protections – originally set out in the 2000 e-Commerce Directive – from liability for the information that they transmit and (depending on their role) for their storage of such information, provided that they respect certain conditions. For example, a digital platform can lose its protection if it becomes aware of illegal content on its platform and does not act expeditiously to remove such content. The Commission has designed a broad framework for the definition of illegal content, including illegal hate speech, terrorist content, unlawful discriminatory content, child sexual abuse material, unlawful non-consensual sharing of private images, online stalking, the sale of counterfeit products, and the non-authorised use of copyright-protected material.

Providers of intermediary services would also continue to have no general obligation to monitor the information that they transmit or store or to actively seek facts or circumstances indicating illegal activity. In contrast to the current regime, providers of intermediary services would not be deemed ineligible for protection from the exemptions from liability solely because they carry out voluntary own-initiative investigations or other activities aimed at detecting, identifying and removing, or disabling of access to, illegal content, or take the necessary measures to comply. In addition, the DSA would impose obligations to cooperate with member states' judicial or administrative authorities in taking action against specific items of illegal content and responding to requests for information about their users.

### Cooperation and enforcement of the Regulation

EU member states would each appoint a DSC with responsibility for all matters relating to the DSA. DSCs would have broadly similar powers of investigation to those enjoyed by the Commission under the DMA, except that maximum fines would be limited to 6% of an intermediary's group worldwide turnover, rather than 10%. Joint investigations by multiple DSCs would be possible.

The DSA Regulation would establish mechanisms for cross-border cooperation between DSCs and the creation of a European Board for Digital Services to assist and coordinate the activities and guidance of DSCs and the Commission. The Commission, for its part, is to have a role in resolving disputes between DSCs regarding investigatory or enforcement measures that should be taken in respect of a particular provider of intermediary services. It would also have its own powers to carry out investigations and impose fines and remedies (broadly the same as the powers available to DSCs) in three circumstances: (i) if a DSC asks the Commission to investigate, (ii) if the Commission considers that a DSC's enforcement or investigatory action is incompatible with the DSA and (iii) where a very large online platform has been found by a DSC to have infringed one of

the obligations that are specific to such platforms (i.e. the fourth layer of obligations described above) and the Commission is not satisfied with the platform's efforts to terminate or remedy the infringement following an "enhanced supervision" process.

## THE LONG ROAD AHEAD

The decision to make both of these proposals Regulations rather than Directives means the DMA and DSA will be directly applicable. It also avoids the additional time that would have been required for national implementation.

Nevertheless, it is still early days for the two proposals and there is a long road ahead before they become EU law.

The two proposals will now be passed to the European Parliament and Council of the EU for adoption under the ordinary legislative process (formerly known as co-decision). Both the Parliament and member states must jointly agree the final wording of the legislation before it can be formally adopted. The timing is difficult to predict but the earliest we can expect final texts to be agreed and adopted is 18-24 months from now, with a further period of 3-6 months before they would become applicable. So it will be a long time before these additional obligations and prohibitions kick in for digital companies in Europe.

It cannot be excluded that the DMA and the DSA might undergo substantial changes as part of that legislative process. What is clear, however, is that

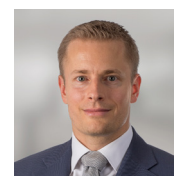
the two proposals have considerable momentum not just at EU level but also among a significant number of EU member states. While there might be a few battlegrounds, such as that between the EU member states and the Commission regarding enforcement competence with respect to the DMA, our view is that the proposals are unlikely to be materially watered down during the legislative process. They might even be further strengthened.

The proposals are also likely to have knock-on effects in other jurisdictions that are considering how to design and implement their own regulatory regimes for the digital sector. Japan has already announced on 16 December that it will look closely at the new European proposals, and we would expect many other countries across the globe to follow suit – including Australia, Brazil, Korea, and Mexico. In the UK, EU law ceases to apply from 1 January 2021, but the Government has advanced plans for its own regulatory regime for certain digital players, to be enforced by a Digital Markets Unit, as well as new legislation regulating online harms and illegal content. And recent antitrust enforcement action by US antitrust agencies against Facebook and Google show that tech giants are also facing stronger policing on their home turf.

The EU's recent proposals may well be the biggest shake-up of the digital sector in recent years, but they are unlikely to be the last.



**There is a stark contrast between the legislation proposed by Brussels and the UK in this area: the UK now has a genuine opportunity to design effects-based, innovation-friendly regulation in the digital space, rather than having to follow the more prescriptive approach from Brussels.**



—**NELSON JUNG**  
Partner, London



# CONTACTS

**Andrei Mikes**  
**Associate, Amsterdam**  
T: +31 20 711 9507  
E: andrei.mikes@cliffordchance.com

**Frans Muller**  
**Counsel, Amsterdam**  
T: +31 20 711 9318  
E: frans.muller@cliffordchance.com

**Jaap Tempelman**  
**Counsel, Amsterdam**  
T: +31 20 711 9192  
E: jaap.tempelman@cliffordchance.com

**Dieter Paemen**  
**Partner, Brussels**  
T: +32 2 533 5012  
E: dieter.paemen@cliffordchance.com

**Anastasios Tomtsis**  
**Partner, Brussels**  
T: +32 2 533 5933  
E: anastasios.tomtsis@cliffordchance.com

**Thomas Vinje**  
**Partner, Chairman, Global Antitrust Group, Brussels**  
T: +32 2 533 5929  
E: thomas.vinje@cliffordchance.com

**Diana Crangasu**  
**Senior Associate, Bucharest**  
T: +40 216666 121  
E: diana.crangasu@cliffordchance.com

**Marc Besen**  
**Partner, Düsseldorf**  
T: +49 211 4355 5312  
E: marc.besen@cliffordchance.com

**Michael Dietrich**  
**Partner, Düsseldorf**  
T: +49 211 4355 5542  
E: michael.dietrich@cliffordchance.com

**Claudia Milbradt**  
**Partner, Düsseldorf**  
T: +49 211 4355 5962  
E: claudia.milbradt@cliffordchance.com

**Joachim Schütze**  
**Partner, Düsseldorf**  
T: +49 211 4355 5547  
E: joachim.schuetze@cliffordchance.com

**Thomas Volland**  
**Partner, Düsseldorf**  
T: +49 211 4355 5642  
E: thomas.volland@cliffordchance.com

**Jörg Rhiel**  
**Partner, Frankfurt**  
T: +49 69 7199 1553  
E: joerg.rhiel@cliffordchance.com

**André Duminy**  
**Partner, London**  
T: +44 207006 8121  
E: andre.duminy@cliffordchance.com

**Joachim Fleury**  
**Consultant to Clifford Chance, London**  
T: +44 207006 8050  
E: joachim.fleury@cliffordchance.com

**Jenine Hulsmann**  
**Partner, London**  
T: +44 207006 8216  
E: jenine.hulsmann@cliffordchance.com

**Nelson Jung**  
**Partner, London**  
T: +44 207006 6675  
E: nelson.jung@cliffordchance.com

**Jonathan Kewley**  
**Partner, London**  
T: +44 207006 3629  
E: jonathan.kewley@cliffordchance.com

**Jennifer Mbaluto**  
**Partner, London**  
T: +32 2 533 5933  
E: anastasios.tomtsis@cliffordchance.com

**Elizabeth Morony**  
**Partner, London**  
T: +44 207006 8128  
E: elizabeth.morony@cliffordchance.com

**Alex Nourry**  
**Partner, London**  
T: +44 207006 8001  
E: alex.nourry@cliffordchance.com

**Greg Olsen**  
**Partner and Head of London Antitrust Practice, London**  
T: +44 207006 2327  
E: greg.olsen@cliffordchance.com

**Simon Persoff**  
**Partner, London**  
T: +44 207006 3060  
E: simon.persoff@cliffordchance.com

**Matthew Scully**  
**Partner, London**  
T: +44 207006 1468  
E: matthew.scully@cliffordchance.com



# CONTACTS

**Jennifer Storey**  
**Partner, London**  
T: +44 207006 8482  
E: jennifer.storey@cliffordchance.com

**Luke Tolaini**  
**Partner, London**  
T: +44 207006 4666  
E: luke.tolaini@cliffordchance.com

**Stavroula Vryna**  
**Senior Associate, London**  
T: +44 207006 4106  
E: stavroula.vryna@cliffordchance.com

**Samantha Ward**  
**Partner, London**  
T: +44 207006 8546  
E: samantha.ward@cliffordchance.com

**Fernando Irurzun**  
**Partner, Madrid**  
T: +34 91 590 4120  
E: fernando.irurzun@cliffordchance.com

**Miguel Odriozola**  
**Partner, Madrid**  
T: +34 91 590 9460  
E: miguel.odriozola@cliffordchance.com

**Claudio Cerabolini**  
**Partner, Milan**  
T: +39 02 8063 4248  
E: claudio.cerabolini@cliffordchance.com

**Gail Orton**  
**Head of EU Public Policy, Paris**  
T: +33 1 4405 2429  
E: gail.orton@cliffordchance.com

**Michel Petite**  
**Avocat of Counsel, Paris**  
T: +33 1 4405 5244  
E: michel.petite@cliffordchance.com

**Dessislava Savova**  
**Partner, Paris**  
T: +33 1 4405 5483  
E: dessislava.savova@cliffordchance.com

**Katrin Schallenberg**  
**Partner, Paris**  
T: +33 1 4405 2457  
E: katrin.schallenberg@cliffordchance.com

**David Tayar**  
**Partner, Paris**  
T: +33 1 4405 5422  
E: david.tayar@cliffordchance.com

**Jan Dobrý**  
**Counsel, Prague**  
T: +420 222 55 5252  
E: jan.dobry@cliffordchance.com

**Luciano Di Via**  
**Partner, Rome**  
T: +39 064229 1265  
E: luciano.divia@cliffordchance.com

**Krzysztof Hajdamowicz**  
**Counsel, Warsaw**  
T: +48 22429 9620  
E: krzysztof.hajdamowicz@cliffordchance.com

**Iwona Terlecka**  
**Counsel, Warsaw**  
T: +48 22429 9410  
E: iwona.terlecka@cliffordchance.com

# CLIFFORD CHANCE

This publication does not necessarily deal with every important topic or cover every aspect of the topics with which it deals. It is not designed to provide legal or other advice.

[www.cliffordchance.com](http://www.cliffordchance.com)

Clifford Chance, 10 Upper Bank Street, London, E14 5JJ

© Clifford Chance 2020

Clifford Chance LLP is a limited liability partnership registered in England and Wales under number OC323571

Registered office: 10 Upper Bank Street, London, E14 5JJ

We use the word 'partner' to refer to a member of Clifford Chance LLP, or an employee or consultant with equivalent standing and qualifications

If you do not wish to receive further information from Clifford Chance about events or legal developments which we believe may be of interest to you, please either send an email to [nomorecontact@cliffordchance.com](mailto:nomorecontact@cliffordchance.com) or by post at Clifford Chance LLP, 10 Upper Bank Street, Canary Wharf, London E14 5JJ

Abu Dhabi • Amsterdam • Barcelona • Beijing • Brussels • Bucharest • Casablanca • Dubai • Düsseldorf • Frankfurt • Hong Kong • Istanbul • London • Luxembourg • Madrid • Milan • Moscow • Munich • Newcastle • New York • Paris • Perth • Prague • Rome • São Paulo • Seoul • Shanghai • Singapore • Sydney • Tokyo • Warsaw • Washington, D.C.

Clifford Chance has a co-operation agreement with Abuhimed Alsheikh Alhagbani Law Firm in Riyadh.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.