The EU Digital Services Act: What does the future hold?

Ben Allgrove
Partner
+442079191788
ben.allgrove@
bakermckenzie.com

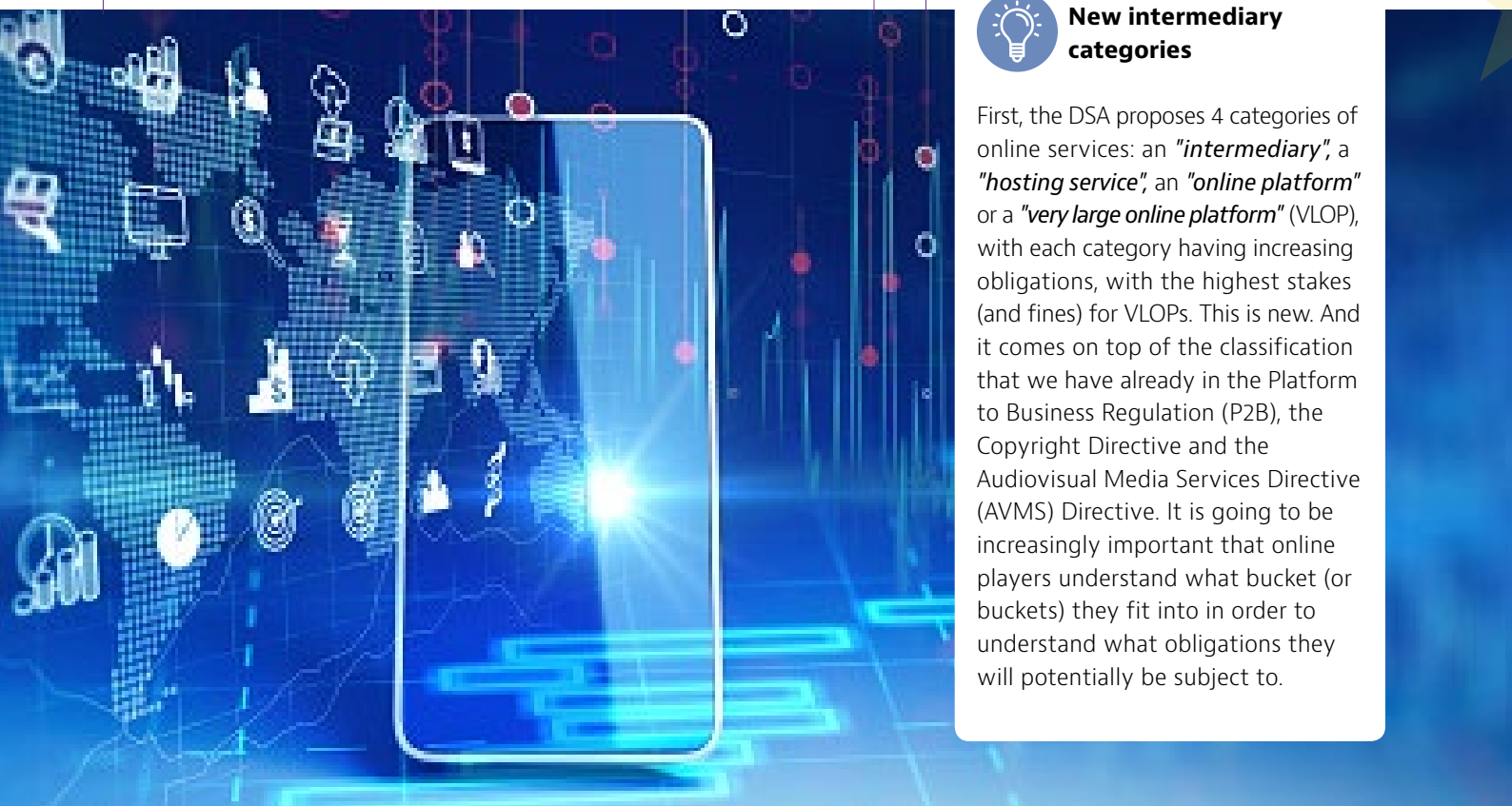
Julia Dickenson
Of Counsel
+442079191237
julia.dickenson@
bakermckenzie.com

Rebecca Bland
Associate
+442079191194
rebecca.bland@
bakermckenzie.com

On 15 December 2020, the European Commission published its long awaited drafts of the "Digital Services Act" (DSA) and "Digital Markets Act" (DMA). In the run up to the drafts being released there was intense speculation about how far the Commission would go in trying to achieve its aims of *"(making) sure that we, as users, have access to a wide choice of safe products and services online. And that businesses operating in Europe can freely and fairly compete online just as they do offline"* (EU Commissioner Margrethe Vestager). Cutting through all the noise, where do the real impacts lie, and what is the road ahead for these high profile Commission proposals?

If you look back at the raft of EU legislative proposals that have come out over the last few years, you can see some common themes in the DSA and DMA, in particular (re)assigning liability or responsibility for online harms and a push for greater transparency from market players.

But what is actually new in the DSA? Some key aspects are covered below and also see the table at the end of this article. For an analysis of the DMA see **here**.



New intermediary categories

First, the DSA proposes 4 categories of online services: an *"intermediary"*, a *"hosting service"*, an *"online platform"* or a *"very large online platform"* (VLOP), with each category having increasing obligations, with the highest stakes (and fines) for VLOPs. This is new. And it comes on top of the classification that we have already in the Platform to Business Regulation (P2B), the Copyright Directive and the Audiovisual Media Services Directive (AVMS) Directive. It is going to be increasingly important that online players understand what bucket (or buckets) they fit into in order to understand what obligations they will potentially be subject to.

Liability and responsibility

Safe harbours

The well-established e-Commerce Directive safe harbours will be largely replicated in the DSA, though with the addition of a "Good Samaritan" provision for intermediaries who carry out investigations to detect illegal content or comply with the DSA. The latter is a change that has long been advocated for by the technology industry and will be welcome. However, the defences will be narrowed to exclude consumer law violations where it is reasonable for consumers to believe the intermediary is providing the information/good/service they have received. In other words, clarity as to with whom a consumer is engaging will become ever more important. This may impact product and customer contracting strategy and structures.

Notice and takedown

The DSA purports to harmonise notice and takedown mechanisms for the first time in the EU. However, the mechanisms proposed are fairly general and in practice are unlikely to materialise into significant changes for the majority of platforms and marketplaces, which mostly already have sophisticated processes in place. The big change proposed is to require a statement of reasons to be provided to explain why a host has removed or disabled content (and to make those statements publicly available). This mirrors a parallel obligation in the P2B Regulation, but with much wider potential impact. We expect to see a lot of discussion about how this might work in practice, and at scale, and how the imperative to provide a safe online experience is balanced against other fundamental freedoms in circumstances which are often highly fact dependent.

Another proposed change is the recognition of "trusted flaggers" which will be specially chosen by (also new) Digital Service Coordinators in Member States, noted for their expertise in flagging illegal content for collective interests. Given some of the current political tensions within the EU about differing member state approaches to the rule of law, we can anticipate that there is likely to be material variance between Member State approaches to trusted flagging.

Know your trader requirements

In an effort to clamp down on illegal and harmful goods and services available online, the Commission also proposes new "know your trader" requirements, making online platforms obtain proof of trader identities and to verify actively whether they are accurate. While some of this information is already collected by platforms, the legal duty to verify it has not been seen before outside of situations where anti-money laundering requirements apply. These requirements echo proposals in other jurisdictions, including in the US, and are a bid by the Commission to make marketplaces take greater responsibility for their platform without – automatically – bearing liability for the actual listings.

VLOPs and "systemic risks"

For the largest platforms, the DSA proposes a requirement for VLOPs to carry out an annual review to identify what "systemic risks" stem from the use and provision of their services and then to take measures to address these risks. This approach invokes the spirit of self-regulation, but with sharper legal teeth, including independent audit.

Transparency/accountability

Transparency reports

One of the strongest themes emanating from the DSA is the push for more transparency. While many intermediaries already provide some, or even much, of the information the DSA is asking for, the draft requires more. All intermediaries must publish transparency reports at least once a year which include the number of orders by Member States to remove content, notice and takedown requests (and the time to remove them) and what content moderation measures they have taken. On top of this, VLOPs must publish details of any automatic means used for content moderation, and the number of disputes submitted to out-of-court dispute bodies and suspensions imposed for misuse of the notice and takedown procedure. All this must be done every 6 months under the eye of a compliance officer appointed by the VLOP, responsible for compliance with the DSA. This seems to be more than what is expected of a Data Protection Officer under the GDPR.

If these reports do not contain information the Digital Service Coordinators (experts appointed by Member States to enforce the DSA) require about VLOPs, there are new broad powers for them to request it. While this can be done already in most Member States via the courts, this is a more direct and potentially more invasive compliance tool. Importantly, there is a proviso that such information does not need to be shared if the VLOP does not have access to the data or if its release might lead to significant vulnerabilities. We expect this to be an area of much debate.

Advertising transparency

If the draft makes it through in its current form, online platforms will have to identify all advertising as such as

well as who is behind the advertising and why that advertising targets certain users. In addition, VLOPs will have to set out the main parameters used in recommendation systems as well as any options for users to modify the influence these have on their use, and to compile and make publicly available information on the content of adverts, who they were aimed at and the total number of recipients reached. These obligations go materially beyond obligations that already exist in most Member States.

The path ahead

The European Parliament and Member States will now discuss the proposed DSA through the ordinary legislative procedure. Reports suggest France wants to reach an agreement during their presidency of the EU Council, which may mean a final DSA Regulation entering into force by the end of 2022.

Ultimately, the date of publication and the final form of the DSA will be dependent on how it fares as it passes through the EU legislative process. It is unlikely to be a smooth ride given some of the implications of the Commission's draft and what we saw with the earlier passage of the Copyright Directive and AVMSD in particular. The US Chamber of Commerce has already said it is "concerned about the direction" of the proposals, suggesting Europe seems "intent on punishing successful companies that have made deep investments in Europe's economic growth and recovery". Such comments will play in the minds of those working on the draft, especially given the wider consequences it might have on transatlantic relationships which the US has flagged "risk being undercut by burdensome and discriminatory proposals".
Key battlegrounds are likely to include the more onerous transparency requirements and additional measures proposed for VLOPs.

We'll keep you updated...

WHAT ARE YOUR OBLIGATIONS UNDER THE DIGITAL SERVICES ACT?

	Intermediary services	Hosting services	Online platforms	Very large online platforms
Transparency reporting (A13, R39)	•	•	•	•
Requirements on terms of service due account of fundamental rights (A12, R3)	•	•	•	•
Cooperation with national authorities following orders (A8 and A9; R29,30,31,32,42)	•	•	•	•
Points of contact and, where necessary, legal representative (A10, R36; A11; R37)	•	•	•	•
Notice and action/obligation to provide information to users (A14 and A15. R40-42)		•	•	•
Complaint and redress mechanism and out of court dispute settlement (A17 and A18, R44 and 45)			•	•
Trusted flaggers (A19, R46 and 47)			•	•
Measures against abusive notices and counter-notices (A20, R46 and 47)			•	•
Vetting credentials of third party suppliers ("KYBC") (A22, R49)			•	•
User-facing transparency of online advertising (A24, R52)			•	•
Reporting criminal offences (A21, R48)			•	•
Risk management obligations and compliance officer (A26, 27 and A32, R57, 59 and 65)				•
External risk auditing and public accountability (A28 and 33, R60, 61 and 65)				•
Transparency of recommender systems and user choice for access to information (A29 and A30, R62 and 63)				•
Data sharing with authorities and researchers (A31, R64)				•
Industry Standards and Codes of conduct (A35 and A36, R66-70)				•
Crisis response cooperation (A37, R71)				•

A — Refers to Articles in the proposed Digital Services Act Regulation **R** — Refers to Recitals in the proposed Digital Services Act Regulation