The EU Digital Services Act: A new era for online harms and intermediary liability

13 February 2023

The EU’s Digital Services Act (DSA) marks the biggest shake up to the rules for online intermediary liability in twenty years.

1. Introduction

The Digital Services Act (DSA)[1] was approved by the Council of the European Union (EU) in September 2022[2] and published in the Official Journal on 27 October 2022.[3]

It marks the biggest shake up to the rules for online intermediary liability in twenty years. The DSA is accompanied by flanking instruments regulating terrorist content, child sexual abuse material (CSAM) and political ads which, together, will create an entirely new framework for the regulation of online harms in the EU.

These new and wide-ranging obligations will attempt to reconcile the damage caused by unregulated user-generated content, fundamental rights to freedom of information, and the practical limitations of moderating content at scale. They will not only be hugely significant to citizens’ online experience within the EU but are also likely to shape the global approach to content regulation in this fast-emerging new area of law.

2. A Determination to Regulate Digital Spaces

The DSA is part of a package of regulation proposed by the European Commission (Commission) to reform digital regulation. This package is notable not only for its ambition but also for the speed of change. The DSA has moved at breakneck speed. Political agreement was reached only eighteen months after it was proposed by the Commission in December 2020, and it is likely to start applying to large social media platforms and search engines in 2023, with the remaining provisions applying in 2024.

Whilst being described as an ‘Act’, this is actually an EU Regulation so will apply directly to every Member State. The DSA imposes tiered obligations so that the more complex and larger the service, the greater the obligations. We summarize these obligations in the table here.

3. Intermediaries Still Protected But Subject to Important New Obligations

3.1 Liability of online platforms


This includes prohibiting any general monitoring obligation from being imposed on these intermediary service providers and preserving the existing ‘notice and takedown’ process – whereby a hosting provider will only become liable for illegal content if, on obtaining actual
knowledge of the illegality, they fail to remove or disable access to the content expeditiously.\[^8\]

Nonetheless, the DSA draws a clearer line between the liability of online platforms and their liability under consumer law. Online platforms, such as marketplaces, will remain liable under consumer law when they lead an ‘average consumer’ to believe that the information, or the product or service that is the object of the transaction, is provided either by themselves or by a recipient of the service who is acting under their authority or control.\[^9\] This will be the case, for example, where an online platform withholds the identity or contact details of a trader until after the conclusion of the contract concluded between the trader and the consumer, or where an online platform markets the product or service in its own name rather than in the name of the trader who will supply that product or service.\[^10\]

When determining whether the online platform created such an appearance, the DSA refers to the concept of ‘average consumer’. This term was analysed by Advocate General Szpunar in the Louboutin case.\[^11\] The Advocate General’s opinion suggests that the marketplace will be liable where a ‘reasonably well-informed and reasonably observant internet user’ perceives the offer of the trader as an integral part of the commercial offer of the marketplace.\[^12\]

Intermediary service providers will also benefit from a new ‘Good Samaritan’ provision under which they will not lose these defences simply because they undertake own-initiative investigations to identify and remove illegal content.\[^13\]

Similarly, where a provider automatically indexes information uploaded to its service, has a search function, or recommends information on the basis of the preferences of the users, it will not be a sufficient ground for considering that provider to have specific knowledge of illegal activities carried out on that platform or of illegal content stored on it.\[^14\]

The preservation of the hosting defence and other intermediary protections is extremely welcome but will now be subject to significant new obligations under the DSA.

### 3.2 Providers of Intermediary Services

All intermediary service providers (including those only providing mere conduit and caching services) must comply with the following requirements:

1. **Single point of contact:** Reflecting the fact that some service providers can be difficult to identify and contact, they must provide a public ‘point of contact’ so they can be contacted by other authorities and users.
2. **EU representative with direct liability:** If a service provider is based outside the EU (but offers services in the EU) it must also appoint a legal representative in the EU. This sounds similar to the EU representative concept in the General Data Protection Regulation (GDPR).\[^15\] However, there is no exemption for small companies.\[^16\] In addition, under the DSA, that representative can be held directly liable for breaches. Given the potentially punitive sanctions (section 6 below), this is not a role to be undertaken lightly. It is not clear if there will be a ready (or cheap) pool of people willing to take on this role, a matter which is highly problematic given the very large number of intermediary service providers subject to this obligation.
3. **Terms and conditions, and disclosure obligations**: The service provider must set out in their terms and conditions any restrictions on the service, alongside details such as content moderation measures and algorithmic decision making.

4. **Annual transparency reports**: The service provider must issue an annual transparency report on matters such as content moderation measures and the number of take down and disclosure orders received.

5. **Acknowledgement of take down and information disclosure orders**: Service providers that receive take down or information disclosure orders from judicial or administrative authorities in the EU must notify the authority of any action taken. However, there is no actual obligation to comply with those orders and their scope and legality will need be separately assessed based on the relevant EU or national law on which they are based. If the service provider takes down the content or discloses information, they must notify the user.

### 3.3 Providers of Hosting Services

Hosting services are a subset of intermediary services consisting of the storage of information provided by or at the request of a user, such as cloud service providers, online marketplaces, social media, and mobile application stores.

In addition to the general intermediary service providers obligations discussed in the previous section 3.1, hosting providers are subject to additional obligations to:

1. **Receive take down requests**: Anyone should be able to notify the hosting provider of illegal content (not just judicial or administrative authorities). The hosting provider must process that notice diligently and report back on whether the content was removed.

2. **Notify users of takedowns**: Hosting providers must notify users if they remove content. This also includes demoting or restricting the visibility of the content (e.g. ‘shadow bans’) and the notification should include details of whether the decision was taken using automatic means (e.g. based on machine learning classifications). However, there is an exception for deceptive high-volume commercial content (more commonly known as spam) reflecting the fact that spam prevention is highly-adversarial. An obligation to automatically notify spammers if their content was identified and removed would simply help them build a better spambot.

3. **Report illegal content**: Hosting providers must inform the judicial authorities if the hosted content creates a suspicion that a criminal offence has occurred – but this is limited to offences involving a threat to life or safety.

### 4. Significant Changes For Online Platforms – Online Harms v. Freedom of Information

The more important changes in the DSA apply to providers of ‘online platforms’. These are hosting providers who, on behalf of a user, store and disseminate information to the public, unless this is a minor and purely ancillary feature. This includes social media services and online marketplaces (but is unlikely to include private messaging services).

Any attempt to regulate user-provided content is fraught with difficulties and raises difficult questions about the balance between fundamental rights to freedom of information, the impact of online harms and the practical limitations attempting to moderate content at scale.
The DSA appears to take a relatively non-interventionist stance. Save for large platforms (section 5 below) there are very limited obligations to police content on the platform. Instead, the new regime appears to have more of a bias to protect content by giving users a right to complain against the removal of content, and even use an out-of-court appeals process if they are unhappy with the platform’s handling of that complaint. This is a significant change for many platforms who will have to be much more transparent about their moderation processes and may need significant additional resources to deal with subsequent objections and appeals from users.

Alongside these changes are other significant new obligations, including:

- **Dark patterns**: Platform providers cannot use interfaces that manipulate or distort the choices taken by users – in addition to those forms of manipulative practices that are already set out in the Unfair Commercial Practices Directive[18] and the GDPR[19].
- **Suspension of repeat offenders**: Where a user continues, after being warned, to ‘frequently’ provide illegal content, the platform provider must suspend them for a reasonable time.
- **Disclosure of monthly active users**: The platform provider must disclose the number of monthly active users in the EU.
- **Advertising and recommender system transparency**: Online platforms shall not present advertising to users based on profiling with special category data. The platform provider must provide users with information about advertisements they are shown including the reasons why that advertisement was selected for them. Where an advertisement is based on profiling, the platform provider must also inform the user about any means available for them to change such criteria. Similarly, the platform provider must be transparent about the operation of any recommender system – i.e. the system used to automatically select content for the user to view.
- **Trader verification**: The platform provider needs to ensure traders on the platform identify themselves and make best efforts to verify certain traceability information before allowing them to use their platforms. The platform will be required to make such information available at least on the interface of its platform to the recipients of the service and in a clear, easily accessible and comprehensible manner. The platform must also design its services to enable those traders to comply with their legal obligations.
- **Online protection of minors**: Providers of online platforms accessible to minors shall put in place appropriate and proportionate measures to ensure a high level of privacy, safety, and security of minors.

While there are some exemptions for small and micro-enterprises, this will be a significant technical and operational lift for many organisations.

**5. Additional Obligations For The Very Largest Platforms**

The highest tier of regulation applies to:

1. **Very large online platforms (VLOP)**: These are very large online platforms which have over forty-five million monthly active users in the EU, a number equivalent to 10% of the EU population, and are designated as such by the Commission.
2. Very large online search engines (VLOSE): These are online search engines which have over forty-five million monthly active users in the EU and are designated as such by the Commission.

This designation brings with it some of the very strongest obligations in the DSA, considering the potential societal impact of such platforms. This includes obligations to conduct a risk assessment of their services and to take steps to mitigate any risks identified as part of that process.

To provide reassurance that appropriate measures have been taken, these entities must also create an independent compliance function and must commission an annual independent audit.

All of this is then backed up by stringent transparency requirements. This includes publishing the independent audit report referred to above alongside other information such as details of the amount of resource dedicated to content moderation. These very large providers must also provide information (including the design, logic the functioning and the testing of their algorithmic systems) to regulators and vetted researchers to allow them to monitor and assess compliance with the DSA.

6. Enforcement

Breach of the DSA comes with the now customary turnover-based fines. It can be punished by a fine of up to 6% of annual worldwide turnover, and users also have a right to compensation for any damage or loss suffered as a result of a breach.

The enforcement mechanism is not only limited to fines. The DSA also allows for enforcement both by national regulators, known as Digital Service Coordinators, and directly by the Commission. They will have the power to require immediate actions where necessary to address very serious harms, and platforms may offer commitments on how they will remedy them.

The Commission will have competence in respect of VLOP and VLOSE, with specific rights for the Commission to charge an annual supervisory fee of up to 0.05% of the provider’s worldwide annual net income to cover its supervisory activities.

7. Application

For most entities, the obligations in the DSA will apply from the later of fifteen months after the DSA comes into force and 17 February 2024.

However, it might start to apply to VLOP and VLOSE from an earlier date as the DSA will apply to them four months after being designated as such by the Commission. Given the Commission is expected to start the designation process soon after adoption, the DSA is expected to apply to these entities in 2023.

8. What Does This Mean For Content Regulation In The EU?

While the DSA forms the cornerstone of the EU’s new content regulation framework, it is accompanied by a number of other new content regulation laws.
The DSA operates by putting in a baseline ‘notice and takedown’ system. As set out above, hosting providers (including online platforms) must allow third parties to notify it of any illegal content it is hosting. Once notified, the hosting provider will need to remove that content expeditiously to continue to benefit from the hosting defence. Added to that, online platform providers must provide an expedited removal process for notifications from trusted flaggers, suspend users who frequently post illegal content and provide additional protection to minors.

Alongside these protections, VLOP and VLOSE have specific obligations to assess and mitigate ‘systemic risks’ arising from their services. That assessment must include the risks of or to:

1. **Illegal content**: This encompasses a wide range of harmful material including CSAM, illegal hate speech, sale of counterfeit or illegal products or services, and illegally-traded animals.
2. **Fundamental rights**: This applies where content would impact on the exercise of fundamental rights, such as freedom of expression, privacy, the right to non-discrimination and consumer protection. Importantly, this does not just mean removing content but also actively supporting free speech by taking measures to counter the submission of abusive take down notices. The rights of a child are particularly important, particularly the risk that minors might be exposed to content that could impair their health, mental or moral development.
3. **Democracy**: This encompasses negative effects on the democratic process, civic discourse and electoral processes, as well as public security.
4. **Gender-based violence and public health**: This includes coordinated disinformation campaigns related to public health (such as some of the recent COVID-19 vaccination disinformation) and interface design that stimulates behavioural addiction.

The DSA is flanked by a number of specific instruments to strengthen and particularise the protections against online harms. For example, illegal content is also regulated by the Regulation on terrorist content online (Terrorist Content Regulation)\[20\] and the proposed Regulation on child sexual abuse (CSAM Regulation).\[21\] These set out a number of specific obligations such as an obligation to remove terrorist content in one hour\[22\] or the ability of authorities to issue detection order to require a provider to install and operate appropriate technology to detect known or new CSAM material\[23\].

There are also specific controls on political advertising in the proposed Regulation on the transparency and targeting of political advertising (Political Advertising Regulation).\[24\] Amongst other things this requires much greater transparency for political advertisements which must be identified as such and contain additional information such as the sponsor of the advertisement and the remuneration for showing the ad.

Finally, this framework will provide extra protection for recognised media sources through the proposed Regulation establishing a common framework for media services (European Media Freedom Act).\[25\] This requires VLOP to allow recognised media sources to declare their status and imposes additional transparency and consultation obligations on VLOP in relation to the restriction or suspension of content from those sources.
9. Emerging Global Content Regulation Laws

The emergence of content regulation laws is not just limited to the EU. There has been an explosion of new laws across the globe including India’s Intermediary Guidelines and Digital Media Ethics Code, Singapore’s Protection from Online Falsehoods and Manipulation Act, and the UK’s Online Safety Bill. Content regulation laws have even been proposed in the US, including the Texas House Bill 20 law, and Florida’s Stop Social Media Censorship Act. However, these laws have generally failed as a violation of the social media companies’ strong rights to freedom of speech under the First Amendment.

While societal factors (such as views on privacy and freedom of speech) have a significant impact on online harms laws, the EU’s position as a ‘regulatory supertanker’ means the DSA is likely to play a pivotal role in the development of other content regulation laws around the world.

10. Online Safety Bill in the United Kingdom

The DSA will not apply to the UK. However, the UK has chosen to implement similar obligations by way of its Online Safety Bill, which was introduced to Parliament in May 2022. This includes placing significant emphasis on conducting risk assessments against a range of different harms.

The Online Safety Bill appears to take a more interventionist approach compared to the EU Digital Safety Act, including the ability of Ofcom (the UK’s communications regulator) to mandate the use of specific content moderation technology. The ‘bells and whistles’ attached to these laws are also very different. For example, the Online Safety Bill contains a range of collateral obligations such as giving users the option to verify their identity and imposing obligations on pornographic websites to block access by children.

The Online Safety Bill has, however, had a difficult passage with significant concerns as to whether it will interfere with freedom of speech. As part of the Conservative leadership campaign earlier this summer, one of the leadership contenders described the Bill as ‘no fit state to become law’ and the provisions to address lawful but harmful content as ‘legislating for hurt feelings’.[26] While the provisions on lawful but harmful material have been dropped to address these concerns, this illustrates the difficult and politically charged issues that arise when attempting to regulate user generated content online.

11. Conclusion

As more and more jurisdictions develop content regulation laws, they are likely to do so in ways that reflect their national traditions and attitudes, particularly the relative importance of free speech compared to privacy, safety and security. While there are, and will continue to be, common themes to this emerging area of law, the global picture looks like it will be fragmented and inconsistent. The obligations in the DSA are summarised in the table here.


The European Parliament and the Council of the European Union adopted the DSA on 5 Jul. 2022 and 29 Sep. 2022, respectively.


A hosting service is defined as the storage of information provided by, and at the request of, a recipient of the service in accordance with Art. 3(g)(iii) of the DSA.

A caching service is defined as the transmission in a communication network of information provided by a recipient of the service, involving the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients upon their request in accordance with Art. 3(g)(ii) of the DSA.

A mere conduit service is defined as the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network in accordance with Art. 3(g)(i) of the DSA.


Art. 6(1), DSA.

Art. 6(3), DSA.

Recital 24, DSA.


Ibid., para. 101.

Art. 7, DSA.

Recital 22, DSA.

Art. 27(2), GDPR.

Art. 3(i), DSA.


Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse (2022/0155(COD)).

Art. 3, Terrorist Content Regulation.

Art. 10, CSAM Regulation.

Proposal for a Regulation of the European Parliament and of the Council on the transparency and targeting of political advertising (2021/0381(COD)).

Proposal for a Regulation of the European Parliament and of the Council establishing a common framework for media services in the internal market (European Media Freedom Act) and amending Directive 2010/13/EU (2022/0277 (COD)).