LATHAM & WATKINS LLP

The EU's Proposed Digital Services Act

New Obligations and Sanctions for Online Platforms

March 2021

Contents

Proposal for the Digital Services Act

The long-awaited update to the e-Commerce Directive proposes new obligations for online platforms and changes to the 'safe harbours' from liability for infringing content

On 15 December 2020, the European Commission released its proposal for a regulation on a Single Market for Digital Services (the Digital Services Act, or DSA) with the aim of amending parts of Directive 2000/31/EC (the e-Commerce Directive) while maintaining its core principles. The DSA applies to intermediary services provided to users (referred to as "recipients of the service" in the DSA) that are established or resident in the EU, irrespective of the place of establishment or residency of the service provider. In the 20 years since the introduction of the e-Commerce Directive, digital services have transformed the lives of EU citizens but there is wide-spread acknowledgement that these new technologies, upon which our society is now dependent, have presented risks and challenges, some of them legal, that could not have been envisioned when the e-Commerce Directive was first introduced. The DSA aims to address certain of these risks and modernise the legislative framework behind digital services in the EU.

Also on 15 December 2020, the Commission published its proposal for a regulation on contestable and fair markets in the digital sector (the Digital Markets Act, or DMA). The DMA proposal targets providers of core platform services (such as intermediation services, search engines, social networks, video-sharing platforms, over-the-top services, operating systems, clouds, and advertising services) who are designated as gatekeepers. The aim is to ensure that markets are contestable and fair in the digital sector across the EU.

Both proposals will now need to go through the EU legislative process, which is likely to be protracted, and could lead to amendments to the draft legislation. The Commission, the European Parliament, and the Council of the EU must reach an agreement on the final texts before the regulations are adopted which may take a number of years. To the extent they are adopted, they will have direct effect in the EU Member States (and will not require implementing legislation).

Liability of Intermediary Service Providers

As expected, the DSA, through Articles 3 to 5, retains the safe harbours from liability for infringing content available under the e-Commerce Directive for intermediary service providers who are mere conduits, or who are caching or hosting information on behalf of users. The hosting safe harbour, however, has been extended to include illegal content (i.e., any information, which in itself or by reference to an activity is not in compliance with EU or Member State law, irrespective of the subject matter of that law) in addition to illegal activities, and made subject to an additional important caveat: this safe harbour expressly does not apply to the consumer protection law liability of online platforms that facilitate consumers entering into distance contracts with traders. Specifically the safe harbour does not apply if online platforms present information or transactions in a way that would lead a consumer to believe that the online platform itself were providing the information or service. The concept of an 'online platform' has been defined by the DSA as "a provider of a hosting service which, at the request of a recipient of the service, stores and disseminates to the public information" subject to the exclusion of incidental and technical functionalities. Online platforms are therefore categorised as a specific type of intermediary service provider (intermediary services being defined as services known as 'mere conduit', 'caching' and 'hosting' services), which is itself a subset of information society services (as defined under the e-Commerce Directive).

The DSA has introduced a welcome clarification in Article 6 on the application of the safe harbours to intermediary service providers who conduct what is referred to as "voluntary own-initiative investigations" aimed at detecting, identifying, and removing access to illegal content". Intermediary service provides will not lose the protection of the safe harbours solely because they choose to conduct such investigations. This clarification should provide service providers with the confidence to engage in such voluntary investigations, although Article 7 reiterates the principle in the e-Commerce Directive that this does not impose a general obligation to monitor on these providers. Articles 8 and 9 further provide that an intermediary service provider must inform any authority that issues an order to "act against" illegal content of the actions it has taken to address such an order. Providers must also provide any information on individual users requested by the authorities, presumably to allow the authorities to assess any liability of any individuals who have uploaded infringing content. In relation to the provision of information on individual users, the recitals to the DSA (which are non-binding, interpretative provisions) state that orders to act against illegal content or to provide information should be issued in compliance with the GDPR; Article 1 also confirms that the DSA is without prejudice to the GDPR.

Through Article 40, the DSA also maintains the e-Commerce Directive principle that the Member State in which the service provider has its main establishment (or in which it has a legal representative where it is established outside the EU, but provides services in the EU, as required under Article 11) shall have jurisdiction for the purpose of enforcing the Regulation against that provider.

Although the safe harbours broadly remain as they were under the e-Commerce Directive, the DSA introduces a number of new obligations for online platforms:

Notice and action mechanisms	Providers of hosting services, including online platforms, are required to implement a notification mechanism whereby any individual or entity can notify the provider of illegal content under the requirements of Article 14. Such mechanisms are already commonly used by global online platforms to comply with laws such as the US Digital Millennium Copyright Act.
Statement of reasons	When a provider of hosting services removes content provided by a user (regardless of how such content was identified), the provider must, in accordance with Article 15, deliver to the user a statement of reasons for its decision to remove such content. Such statement of reasons should contain (amongst other information): • Information on whether content has been removed or disabled, and if relevant, the territorial scope of disabled access • The facts relied upon in taking the decision • Information on the redress mechanisms available to that user.
Internal complaint-handling system	Under Article 17, users must be provided with access to an effective internal complaint-handling system that allows users to lodge complaints, electronically and free of charge, against decisions to either: • Remove or disable access to content • Suspend the provision of the services to users s (presumably the provider(s) of the offending content) • Suspend or terminate a user's account, if such decision was taken by an online platform on the basis that the service was being used to transmit illegal content or content incompatible with the platforms terms and conditions.

Trusted flaggers	Necessary technical and organisational measures need to be implemented to ensure that notices submitted by trusted flaggers under Article 14 are processed without delay. Article 19 further sets out how trusted flaggers can be appointed by the Digital Services Coordinator of a Member State.
Protection against misuse	Under Article 20, online platforms shall, after issuance of a warning, suspend the provision of their services to users that frequently provide manifestly illegal content and suspend the processing of notices submitted by users that frequently submit manifestly unfounded notices.
Traceability of traders	Under Article 22, if an online platform facilitates consumers concluding distant contracts with traders, it shall ensure that traders can only use its services to promote their products and services if the online platform has been provided with certain information about that trader (such as name, contact details, bank account details, relevant identification documentation, and trade registers) and such information has been confirmed to be reliable. If such information is inaccurate or incomplete, the trader must provide corrected information or the online platform must suspend the provision of services to the trader.

Transparency

A number of new transparency obligations have been introduced for intermediary service providers, including the following.

- Article 10 requires intermediary service providers to identify a single point of contact allowing for direct communication with Member State authorities, the Commission, and the new European Board for Digital Services (the Board).
- Article 11 requires intermediary service providers that are not established in the EU, but which offer services into the EU, to designate a legal representative in a Member State in which it is offering its services for the purpose of receipt of, compliance with, and enforcement of decisions issued under the DSA. Such legal representative can be held liable for non-compliance with the DSA without prejudice to the liability that could be initiated against the service provider.
- Article 13 requires intermediary service providers to, on at least an annual basis, publish a comprehensive report on any content moderation that they engaged in during the relevant period. Such reports do not apply to providers that qualify as micro enterprises (i.e., those with fewer than 10 employees and whose annual turnover does not exceed €2 million) or small enterprises (i.e., those with fewer than 50 employees and whose annual turnover does not exceed €10 million).
    - Article 24 requires online platforms to ensure that users can identify the following in real time, for each advertisement displayed:
    - That the information displayed is an advertisement
    - The natural or legal person on whose behalf the advertisement is displayed
    - The parameters used to determine whom that advertisement is displayed to

The Article 24 obligations are intended to sit alongside those under the General Data Protection Regulation (GDPR) regarding profiling and the right to object to direct marketing, as well as the e-Privacy Directive's cookies rules. No clarity has been provided around the obligation to provide information on the parameters that determine whom an advertisement is displayed to. Depending on how this requirement is interpreted, the operation of adtech companies could be significantly impacted.

Very Large Online Platforms

Very large online platforms (i.e., those with at least 45 million active monthly users in the EU, as can be adjusted for changes in the EU population) are subject to additional obligations to manage so-called systemic risks as set out in Articles 26 and 27. Such platforms are required to conduct an annual assessment on any significant risks stemming from the functioning and use of their services, including the following systemic risks:

- Dissemination of illegal content
- Any negative effects for the exercise of the fundamental rights for private and family life, freedom of expression and information, the prohibition of discrimination, and the rights of the child as set out in the EU's Charter of Fundamental Rights

- Intentional manipulation of their service with an actual or foreseeable negative effects on the protection of public health, minors, civic discourse, or related to electoral processes and public security

Very large online platforms must consider how these risks are impacted by their content moderation systems, so called "recommender systems", and systems for displaying advertisements. They must then implement reasonable and proportionate mitigation measures to address the systemic risks identified. Such measures could include adapting internal systems, the functions of the service, or the terms and conditions for use of their service.

Very large online platforms are subject to a range of other obligations, including requirements to:

- Submit to annual independent audits to confirm their compliance with various obligations under the DSA (Article 28): Such audits must cover compliance with the obligations of Chapter III and commitments undertaken pursuant to the codes of conduct referred to in Articles 35 and 36, and the crisis protocols in Article 37. The organisation performing such audit must be independent of the platform concerned, have proven expertise in risk management, possess technical competence, and have proven objectivity and professional ethics. At a minimum, the reports must include:
    - The name, address, and point of contact of the platform concerned and period covered by the audit
    - The name and address of the auditor
    - A description of the specific elements audited and methodology applied
    - A description of the main findings of the audit
    - An opinion (either positive, positive with comments, or negative) on whether the platform concerned has complied with the relevant obligations and commitments

      If the opinion of the auditor is not positive, the report must also provide operational recommendations on specific measures to achieve compliance. Within one month of receiving such recommendations, the platform must adopt an audit implementation report setting out the remedial measures to be implemented. If those measures were not implemented, it should provide justifications for not doing so and any alternative measures taken to address the non-compliance.
- Provide the Digital Services Coordinator or the Commission with access to data necessary to monitor compliance with the DSA (Article 31): Such data is to be provided through online databases or application programming interfaces, and the Commission shall adopt delegated acts laying down the technical conditions under which such data should be shared. It remains unclear how platforms will balance this disclosure obligation against their obligations under the GDPR to the extent such data contains personal information.

Separately, the Commission and the Board shall facilitate the drawing up of codes of conduct, including for online advertising, taking into account the specific challenges of tackling different types of illegal content and systemic risks in accordance with competition and privacy laws. Online platforms and other interested parties may be invited to participate in the preparation of such codes of conduct.

Sanctions

Each Member State is permitted to determine the penalties applicable to infringements of the DSA by providers of intermediary services under their jurisdiction, with the maximum penalty for failure to comply with the DSA not to exceed 6% of that intermediary service provider's total annual income or turnover (although it's not clear whether this refers to global turnover or the turnover in the jurisdiction of that Member State). The proposal therefore provides significant fining powers to Member States, which may result in much greater enforcement risk for providers, depending on how those powers are ultimately utilised in practice.

The Commission may impose periodic penalty payments (not exceeding 5% of the average daily turnover of the preceding financial year) on very large online platforms to compel such platforms to:

- Supply accurate and complete information in response to the Commission's request for information
- Submit to on-site inspections ordered by the Commission
- Comply with a decision ordering interim measures to be implemented
- Comply with legally binding commitments offered by such platforms during proceedings
- Comply with any non-compliance decisions adopted by the Commission if it finds that the platform is not complying with the obligations of the DSA, any interim measures ordered upon it, or its legally binding commitments

In addition to financial penalties, Digital Services Coordinators may conduct on-site inspections of service providers and adopt interim measures to avoid the risk of serious harm. In the most serious cases, in which other options to stop the infringement have been exhausted and recurrent infringements relate to serious criminal offences, Digital Services Coordinators may request a competent judicial authority to order the temporary restriction of access to the service. If that option is not technically feasible, they may instead request a competent judicial authority to order the temporary restriction of access to the online interface of the service provider on which the infringement occurs.

French-specific Considerations

France has been a strong supporter of the DSA and the DMA. This position is reflected in the current administration's emphasis on the need to reinforce ex ante regulation of very large online platforms and to strengthen accountability mechanisms. Shortly after the Commission's publication of the proposals, the French government published a press release conveying France's willingness to support the upcoming negotiations and legislative work. The press release also noted that France would aim to adopt those elements of the package that require national implementation by early 2022.

In parallel, France stayed the adoption of its draft national law to enhance consumer choice online to give priority to the EU legislative process. The recent announcement regarding the collection of the 3% digital services tax that targets companies active in the digital sector, regardless of their location, with annual of taxable revenues of more than €25 million in France and €750 million worldwide, is another example of France's strong political will further to regulate large digital players.

The e-Commerce Directive has been transposed into French national law through Law No. 2004-575 of 21 June 2004 regarding trust in the digital economy that included amendments to the French Consumer Code and the Law No. 86-1067 of 30 September 1986 regarding freedom of communication. As such, further amendments to these texts can be expected should the DSA be adopted. The French Consumer Code already imposes significant transparency obligations specific to platforms and online publicity, partly pre-empting the obligations the DSA seeks to introduce. Similarly, recent legislative efforts regarding online content regulation, such as the Law No. 2020-766 of 24 June 2020 on online hate speech, have been aiming to clarify the existing liability regime regarding intermediary service providers. The impact on the French regulatory landscape is therefore expected to be moderated by pre-existing legislation and various preparatory works.

German-specific Considerations

The DSA will be directly applicable in Germany once it has been finally adopted so that generally no implementing legislation is needed. However, the DSA replaces certain existing legislation which implements those parts of the e-Commerce Directive that it supersedes — namely, the liability exemptions in the Germen Telemedia Act (Telemediengesetz). Further legislative changes may therefore be required. For example, the notice and action mechanism regarding illegal content in Article 14 of the DSA is similar to a complaint handling mechanism set out in the German Network Enforcement Act (Netzwerkdurchsetzungsgesetz, NetzDG).

As the legislative proceeding concerning the DSA is still at an early stage, it remains to be seen how the legislative environment in Germany will be affected. Apart from a recent press release by the German Federal Ministry for Economic Affairs and Energy welcoming the DMA, no official statement on the DSA and its implementation in German law has been issued.

UK-specific Considerations and Brexit

The DSA will not be applicable to the UK given that new EU rules introduced after 31 December 2020 will not be adopted into UK law. The e-Commerce Directive does, however, remain applicable in its current form under UK law through the Electronic Commerce (EC Directive) Regulations 2002. The UK government has confirmed that there are no current plans to amend the UK's intermediary liability regime or its approach to the prohibition on monitoring. However, current proposals for the UK online harms regime suggest that there may be tension regarding this point. This leaves questions over the position of intermediary service providers in the UK and their exposure under the e-Commerce Directive in the event that they implement "voluntary own-initiative investigations".

The UK, however, is in parallel in the process of introducing an online harms regime aimed at controlling the spread of illegal and harmful online content. The proposed regime will apply to website operators whose websites include functionality for user-generated content and user interaction. Under the proposed regime, the regulator, Ofcom, will be empowered to impose fines of up to £18 million or 10% of global turnover. Further, the UK has proposed setting up a new Digital Markets Unit (which will form part of the Competition and Markets Authority, and which will work closely with other regulators such as Ofcom and the Information Commissioner's Office) that will regulate and enforce new UK competition laws for online platforms.

Contacts

Jean-Luc Juhan
Partner, Paris
T +33.1.40.62.23.72
E jean-luc.juhan@lw.com

Deborah J. Kirk
Partner, London
T +44.20.7710.1194
E deborah.kirk@lw.com

Elisabetta Righini
Partner, Brussels
T +32.2.788.6238
E elisabetta.righini@lw.com

Thies Deike
Counsel, Frankfurt
T +49.69.6062.6508
E thies.deike@lw.com

Grace E. Erskine
Associate, London
T +44.20.7710.1835
E grace.erskine@lw.com

Alain Traill
Associate, London
T +44.20.7710.4737
E alain.traill@lw.com

Amy Smyth
Knowledge Management Lawyer, London
T +44.20.7710.4772
E amy.smyth@lw.com