CLIFFORD
CHANCE

THE DIGITAL SERVICES ACT – WHAT IS IT AND WHAT IMPACT WILL IT HAVE?

THE DIGITAL SERVICES ACT – WHAT IS IT AND WHAT IMPACT WILL IT HAVE?

The Digital Services Act (DSA) entered into force on 16 November 2022, creating new standards for digital services in the EU. The DSA regulates providers of online "intermediary services", such as cloud providers, online marketplaces and app stores. The harmonised rules it introduces are broad and include provisions affecting illegal online content moderation, transparency requirements, user rights and protections and provider liability.

The DSA, together with its sister regulation, the Digital Markets Act (DMA) which came into force on 1 November 2022, will form a set of new rules intended to create a safer and more open digital space and to foster innovation and competitiveness.

What is the DSA?

The DSA is a regulation that will transform and harmonise the EU's legal framework. The rules reform and supplement the e-Commerce Directive as it relates to online intermediaries, maintaining core pillars such as safe harbour provisions while introducing a host of new obligations relating to disinformation, illegal goods and content, cyber violence, dark patterns and targeted advertisements.

Businesses operating online will benefit from access to tools for flagging illegal content and activities that could otherwise damage their trade, as well as from redress mechanisms for challenging the erroneous removal of content.

Failure to comply with the DSA may, in serious cases, result in fines of up to six percent of annual global turnover. Lesser breaches, such as the provision of incorrect or misleading information to regulators, may result in fines not exceeding one percent of annual turnover.

The DSA applies alongside its sister regulation, the DMA, which will impose a long list of obligations and prohibitions on digital platforms that are designated as "gatekeepers", seeking to ensure fair and contestable digital markets in the EU. Each is a core component of the EU's wide-reaching reform of digital sector regulation and, in combination, the two pieces of legislation create a strong regulatory regime for the digital sphere in Europe. Core components of the DSA focus on online content regulation and user protection, while the DMA seeks to prevent large and influential digital companies from implementing practices that are considered to limit competition or to otherwise be unfair.

The DSA, as horizontal and widely applicable legislation, will also be complemented by voluntary codes, such as the **2022 Code of Practice on Disinformation**, and vertical legislation for specific activities or sectors, such as the **proposed legislation on Transparency and Targeting of Political Advertising**.

The DSA introduces wide-ranging obligations on intermediary services providers and new rights for users, including:

- updating the regime for intermediary liability for third-party content;
- rules to trace sellers on online platforms allowing consumers to conclude distance contracts with traders;
- mechanisms to address illegal content, goods and services;
- increased rights for users, including to challenge content moderation decisions;
- increased transparency requirements for online platforms;
- obligations for the protection of minors;
- new limits on targeted advertising.

The complexity of the EU's emerging digital regulation framework becomes evident when you apply these requirements in practice. National laws need to be considered alongside existing and proposed EU-wide laws. They need to be considered holistically when business strategies, operations and tools are created or reviewed.

DESSISLAVA SAVOVA
Partner

To whom will the DSA apply?

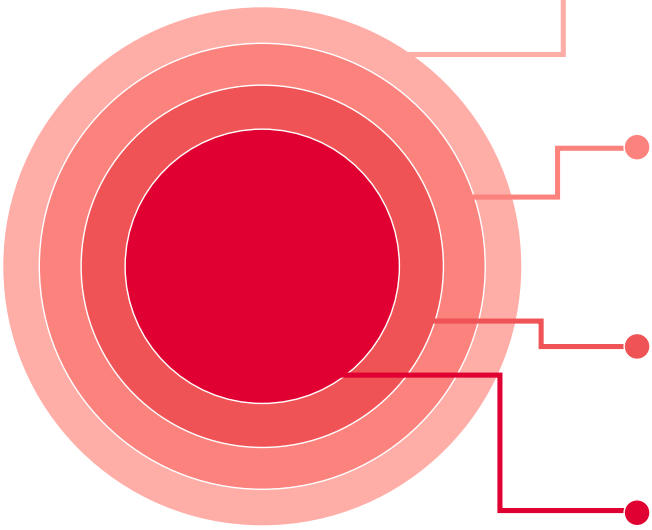
The DSA will apply to a range of providers of digital "intermediary services", where such services are offered to natural or legal person recipients that are established or located in the EU. In practice, this catches a broad range of businesses which store or transmit the content of third parties, including internet service providers, providers of web-based messaging services and email services, providers of cloud computing or web hosting services, social media networks, app stores, online marketplaces and online search engines. Note that the concept of "offering" services is broad under the DSA, with providers of intermediary services caught if they enable use of their service by EU users and have a "substantial connection" to the EU, such as targeting activities towards a Member State.

The rules are "tiered", with certain lower-level obligations applying to network infrastructure providers and hosting services, whilst online platforms like marketplaces and apps stores attract more stringent regulation. The strictest rules are reserved for "Very Large Online Platforms" (VLOPs) and "Very Large Online Search Engines" (VLOSEs) that reach more than 45 million active EU service recipients on average each month and are designated as VLOPs or VLOSEs under the DSA. For example, VLOPs will be obliged to undertake systemic risk assessments and mitigate the risks posed by the intentional manipulation of their platforms by users. Whilst many of the liability "safe harbours" set out in the e-Commerce Directive are largely preserved, the active steps that VLOPs and VLOSEs (and other intermediaries) must take to comply with the DSA raises the compliance bar considerably.

VLOPs and VLOSEs that meet the DSA's threshold of 45 million active EU users might also satisfy one of the DMA's three cumulative criteria for being designated as a "gatekeeper". If a VLOP or VLOSE were to be designated as a "gatekeeper" under the DMA, it would have a number of additional obligations and prohibitions to comply with the DMA. For further information about the DMA's designation criteria for gatekeepers, please see **The Digital Markets Act: A new era for the digital sector in the EU**.

Under the DSA, intermediary services are any of the following:

- "mere conduit" services – i.e. transmitting information from a service recipient via a communications network, or providing access to a communications network;
- "caching" services – i.e. the automatic, intermediate and temporary storage of information provided by a service recipient through a communication network in order to make its further transmission more efficient; and
- "hosting" services – i.e. the storage of information provided by, and at the request of, a service recipient.



Tier 1: Intermediary Services
all providers of intermediary services (including 'mere conduits' and providers of 'caching' and 'hosting' services), regardless of further sub-classification under any other tier.

Tier 2: Hosting Services
a type of intermediary services that involves the storage of information provided by (and at the request of) a service recipient, e.g., web hosting and cloud services.

Tier 3: Online Platforms
a type of hosting service which, at the user's request, stores and makes publicly available user-provided information, e.g., social media platforms and online market places.

Tier 4: Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs)
online platforms and online search engines with more than 45 million active EU users on average each month.

What are the key obligations for different types of providers?

Intermediary service providers

Intermediary services, in the broadest sense, are subject to the first "tier" of DSA obligations. This creates a set of "baseline" obligations to which all intermediary service providers are subject. The other provisions of the DSA then apply in layers to certain types of intermediary service providers.

Obligations applicable to all providers of intermediary services include:

Ts&Cs, transparency and reporting: All providers of intermediary services will be obliged to review their Ts&Cs to ensure certain minimum requirements are met, particularly with regard to clarity, transparency and fairness, and that they include information on any policies, procedures, measures and tools used for content moderation. They will also be subject to an annual transparency and reporting regime (unless they are SMEs) in relation to their content moderation actions.

EU representative: Any intermediary service providers without an EU establishment (but who offer services in the EU) must designate a local representative in one of the EU Member States where it operates. That representative can be held liable for non-compliance with DSA obligations, albeit without prejudice to actions that could also be initiated against the provider itself.

Hosting service providers (including online platforms)

Notice and action mechanisms: The DSA sets a number of requirements for intermediary service providers that provide hosting services, which apply in addition to the "baseline" obligations. These include greater responsibility on hosting providers to provide user-friendly notice and take-down mechanisms that allow notification of illegal content by third parties. The chosen mechanism must enable individuals or entities to submit detailed notices that would enable the hosting provider to identify whether the notified information is illegal or incompatible with their terms and conditions without conducting a legal or factual examination. Once received, the hosting service provider must process the notice and swiftly decide on possible action (for example, to remove or disable access to the content) and inform the notifier of the measures taken. It remains to be seen whether a 'delete first, think later' approach will emerge among providers, given the resources required to assess allegations made under the notice-and-action regime.

Some of the obligations imposed by the DSA already exist in certain Member State laws. For example, in France, hosting service providers and providers of access to online communication networks are already subject to notice and action mechanisms requirements in relation to certain types of illicit content. Similarly, various German national laws, such as the *NetzDG* (*Netzdurchsetzungsgesetz*) and the *UrhDaG* (*Urheberrechts-Diensteanbieter-Gesetz*), include obligations to set up a notice mechanism. Consequently, commonly used instruments to address such requirements already exist among such providers, not least to comply with US law requirements, such as the US Digital Millennium Copyright Act. However, the DSA provides for more detailed rules and it remains to be seen whether there will be any parallel application of such laws.

Online platforms

Hosting services which fall within the definition of "online platforms" face greater requirements still, in addition to those referenced above. There are additional reporting obligations for all providers of online platforms. Subject to an exception for micro and small enterprises, other additional obligations include:

Balancing complaints and freedom of speech: Online platforms (other than micro or SME platforms) will be required to set up an internal complaint-handling system that enables service recipients whose information has been affected by certain content moderation decisions to lodge electronic complaints within a given time period. Following the complaint, the online platform must review the decision, and potentially reverse it if the content is legitimate. These decisions are not supposed to be taken on the basis of automated means only, i.e. qualified staff will be needed to ensure compliance, which will likely involve a certain bureaucratic effort as well as a noticeable cost burden for the providers.

Traders' traceability and obligations regarding illegal products and services: Online platforms which allow consumers to enter into online contracts with traders must ensure that such traders have provided certain information to ensure their traceability and must check the information provided to the best of their ability. If an online platform becomes aware that any traders offer illegal products or content, it must remove these and keep a record of such removal, as well as fulfil certain information requirements in respect of its customers, consumers in general and the relevant authorities.

Online advertising: Building on the foundations of the e-Commerce Directive (which already required commercial communications and the entity sending them to be clearly identified), the DSA requires platforms to clearly identify (1) the parameters they use to determine the receipients to whom the advertisement is presented, and (2) how to change those parameters. In practice, publishing such information about the logic underlying complex targeted advertising processes may prove challenging, not least because of the layers of information requirements that can apply under various laws. For example, if personal data and data generated by connected devices were to be processed using AI by an online platform for targeted advertising purposes, information requirements under the GDPR, the proposed Data Act and the proposed AI Act could apply, alongside those imposed by the DSA.

In addition, the DSA takes a narrower view than the GDPR in certain respects – for example, implying that consent is the only legal basis for processing personal data for online advertising, and prohibiting the presentation of advertising based on profiling using special categories of personal data or where the service recipient is a minor.

The DSA's rules also complement the DMA's provisions requiring "gatekeepers" to provide advertisers and publishers to which they supply online advertising services with information about prices paid and remuneration received, as well as the methodology under which the prices and remuneration were calculated.

The obligations relating to traceability and illegal products are not entirely new as most e-commerce platforms and marketplaces already have a degree of 'know your customer' requirements in place to comply with existing legislation, such as anti-money laundering laws, the e-Commerce Directive and the transfer of funds directive. Placing the DSA in the context of existing regimes will be essential in order to ensure alignment and maintain clarity and practicability for traders and marketplace providers.

FLORIAN REILING
Counsel

Recommender system transparency: Recommender systems – being software which predicts a user's preference – are responsible, for example, for generating 'Made for you' playlists, 'Similar products' lists and 'Films you may like' options. The DSA requires that online platforms and search engines recommending content must provide users with easily accessible information regarding how the recommender system operates (including its criteria, parameters, any objectives and how the user's behaviour affects output) and the options available to modify or influence these parameters. While the DSA does not impose a mandatory 'disable recommendations' option, it does require that online platforms make it easy for users to modify the parameters of recommender systems. The DSA does not, however, tackle the possibility of bias or discrimination in recommender system logic, leaving this for other legislation (including the proposed AI Act) to prevent.

Online interface designs and "dark patterns": Importantly, online platforms will be prohibited from using the structure, function or manner of operation of their interfaces to distort or impair recipients' ability to make informed decisions – including specific restrictions on repeatedly inviting users to consent to processing or making termination more cumbersome than "signing up". Design features must also ensure a high level of privacy, safety and security by design for minors. These requirements echo and build on transparency, consent and privacy by design requirements in the GDPR, and will need to be considered alongside the evolving body of guidance published by privacy authorities in relation to the processing of data relating to minors.

Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs)

Systemic risk assessment obligations & risk mitigation

The DSA reserves the strictest rules for VLOPs and VLOSEs. For example, they must effectively and diligently identify the systemic risks stemming from the use of their services, particularly where those risks relate to the sharing of illegal content or where content generates an actual or foreseeable negative effect on users' fundamental rights. For example, where the intentional manipulation of their services may have certain types of actual or foreseeable negative effects (such as negative effects on democratic processes, electoral processes or public security), those risks must be proactively mitigated. Such mitigation measures include adapting moderation processes, reinforcing supervision of their activities, and other steps which, arguably, come close to qualifying (if not contradicting) the general proposition that intermediaries are not obliged to actively monitor third-party content.

There is an unmistakable trend toward increased transparency requirements in the use of technology and data, both in the activity of national courts and regulators in Europe and in proposed EU regulation such as the AI Act and the Data Act. The DSA imposes prohibitions intended to protect certain vulnerble groups, as well as more generally imposing heightened transparency requirements on online plaforms which host targeted advertising content.

ANDREA TUNINETTI FERRARI
Counsel

How does the DSA compare with the UK's proposed Online Safety Bill (OSB)?

The UK's OSB introduces rules for firms which host user-generated content. Applying more narrowly than the DSA, the OSB specifies direct obligations for providers of user-to-user services and search engines. Service providers will be classified into different categories based on number of users and risk profiles. Enforcement powers of the regulator, Ofcom, could include fines of up to £18m or 10% of global revenue and criminal sanctions against senior managers in certain circumstances.

Key similarities between the DSA and OSB include: (1) both introduce responsibilities relating to risk assessments for illegal content, and requirements around mitigation and management of the risks of harm to individuals in certain circumstances (including obligations relating to content moderation and design or functioning of algorithms); (2) specific obligations on services that are likely to be accessed by children; and (3) a duty for certain companies to minimise the likelihood of fraudulent advertisements being published on their service.

Key differences include: (1) the OSB not only regulates illegal content, but also the largest high-risk platforms must address categories of "legal but harmful material", a phrase that lacks clarity but could include issues such as abuse, harassment and content encouraging self-harm; and (2) unlike the DSA, the OSB does not address illegal products and services or trader traceability.

How will the DSA be enforced?

Member States will each designate a 'Digital Services Co-ordinator' (DSC) to ensure the supervision and enforcement of the DSA (including in relation to fines), and may also designate other competent authorities with specific roles. The DSA establishes a one-stop-shop mechanism for cross-border infringements, and a GDPR-like supervisory structure, establishing a European oversight and advisory entity – the European Board for Digital Services (EBDS) – which would be composed of the national DSCs. Unlike the GDPR's European Data Protection Board, the EBDS would be chaired by the Commission. The increased importance of the Commission's role in supervision and enforcement of the DSA is particularly evident when it comes to the supervision of VLOPs and VLOSEs. Notably, the Commission has exclusive powers to supervise and enforce the subset of obligations that only apply to VLOPs and VLOSEs.

Beyond ensuring uniform implementation of these requirements, granting the Commission some exclusive supervisory and enforcement powers was also likely a move to limit the concentration of the enforcement of the DSA in countries such as Ireland and Luxembourg, where the majority of tech companies that could qualify as Very Large Online Platforms are likely to have their European headquarters, and consequently limit the chances of having complaints mounting up with the regulators of those countries.

Such mitigation measures include moderation processes, reinforcing supervision of their activities, and other steps which, arguably, come close to qualifying (if not contradicting) the general proposition that intermediaries are not obliged to actively monitor third-party content.

MICHAEL EVANS
Counsel

When will the DSA start to apply?

The DSA will be directly applicable across the EU and will start to apply from 17 February 2024. Exceptions to this include obligations for online platforms to disclose the number of their average monthly active recipients, which will start to apply from 17 February 2023, and the rules governing VLOPs and VLOSEs which will apply from four months after the relevant service provider is notified by the Commission that it has been so designated where that date is earlier than 17 February 2024.

How can businesses prepare for the DSA?

Key steps in preparing for the DSA's application include:

- **Services mapping:** Businesses whose services may fall within the broad definition of intermediary services should assess their services against the DSA definitions and keep watch for guidance which may be issued by relevant authorities to further clarify the intermediary services classifications.
- **Identifying appointments:** The DSA contains several obligations related to the designation of points of contact, legal representatives and compliance officers, as applicable. In-scope businesses should therefore anticipate and determine the natural (or, where permissible, legal) persons to be designated, taking into account any requirements such as independence, qualifications and seniority, where applicable. More generally, they should carry out a strategic review of their governance processes, and also consider how these functions under the DSA interact with roles under other existing or upcoming tech regulations.
- **Reviewing documents, processes, tools and interfaces:**
  - The DSA imposes specific obligations related to the content, format and accessibility of certain documents and information, such as terms and conditions.
  - Certain in-scope businesses now face new requirements for specific mechanisms (such as notification tools for illegal content or recourse mechanisms allowing the challenge of content moderation decisions) and/or reports. For instance, online platforms are obliged to publish reports on their content moderation activities and regularly disclose information on their number of average monthly active recipients. These obligations require efficient internal mechanisms, including for information gathering.
  - Importantly, some businesses will need to prepare for obligations requiring the adaptation of the design, presentation and/or functioning of their online interfaces.
  - VLOPs and VLOSEs also need to assess the systemic risks relating to the functioning and use of their services, implement any necessary measures to mitigate those risks, and be prepared to demonstrate compliance in the context of the mandatory independent audits.

Overall, preparing for, and keeping up with, the new DSA requirements will entail additional efforts and investments, as well as technical and human resources that businesses should anticipate.

Companies will have started looking at the draft DSA and considering what it may imply, at least for their core businesses. This was a useful and necessary step. Now, it is time to ramp up the DSA compliance readiness work: pursuing the necessary assessments and gap analyses, and planning ahead – including in terms of expected governance and preparing for the possible adjustment of systems, processes and documentation.

ALEXANDER KENNEDY
Counsel

CONTACTS

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

Dr. Thomas Voland
Partner
Düsseldorf
T: +49 211 4355 5642
E: thomas.voland@cliffordchance.com

Josep Montefusco
Partner
Barcelona
T: +34 93 344 2225
E: josep.montefusco@cliffordchance.com

Rita Flakoll
Senior Associate Knowledge Lawyer
London
T: +44 207006 1826
E: rita.flakoll@cliffordchance.com

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

Gunnar Sachs
Partner
Dusseldorf
T: +49 211 4355 5460
E: gunnar.sachs@cliffordchance.com

Dr. Michael Dietrich
Partner
Dusseldorf
T: +49 211 4355 5542
E: michael.dietrich@cliffordchance.com

Jaap Tempelman
Senior counsel and co-head of Tech Group
Amsterdam
T: +31 20 711 9192
E: jaap.tempelman@cliffordchance.com

Andrea Tuninetti Ferrari
Lawyer - Counsel
Milan
T: +39 02 8063 4435
E: andrea.tuninettiferrari@cliffordchance.com

Victoria Baltrusch
Knowledge Lawyer
Paris
T: +33 1 4405 5134
E: victoria.baltrusch@cliffordchance.com

Alexander Kennedy
Counsel
Paris
T: +33 1 4405 5184
E: alexander.kennedy@cliffordchance.com

Dr. Florian Reiling
Counsel
Düsseldorf
T: +49 211 4355 5964
E: florian.reiling@cliffordchance.com

Preslava Eneva
Avocat
Paris
T: +33 1 4405 5379
E: preslava.eneva@cliffordchance.com

Susanne Werry
Counsel
Frankfurt
T: +49 69 7199 1291
E: susanne.werry@cliffordchance.com

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

Kelly Cannon
Avocat
Paris
T: +33 1 4405 5350
E: kelly.cannon@cliffordchance.com

Michael Evans
Counsel
London
T: +44 207006 1757
E: michael.evans@cliffordchance.com

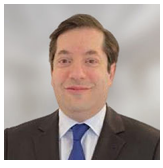
Arnav Joshi
Senior Associate
London
T: +44 207006 1303
E: arnav.joshi@cliffordchance.com

Linda Agaby
Lawyer
London
T: +44 207006 3125
E: linda.agaby@cliffordchance.com

Eliot Cohen
Lawyer
London
T: +44 207006 2966
E: eliot.cohen@cliffordchance.com

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

Vanessa Marsland
Partner
London
T: +44 207006 4503
E: vanessa.marsland@cliffordchance.com



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

Megan Gordon
Partner
Washington DC
T: +1 202 912 5021
E: megan.gordon@cliffordchance.com

Ling Ho
Partner
Hong Kong
T: +852 2826 3479
E: ling.ho@cliffordchance.com

CLIFFORD

CHANCE

www.cliffordchance.com

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

2212-004095