The Digital Services Act, Countdown to Compliance: What Do Brands Need to Know and Do?

INTA Data Protection Committee, Education & Awareness Subcommittee

Chair: Philip V. Marano (Greenberg Trauring LLP)

Vice Chair: Nicola Benz (MLL Legal)

Subcommittee Chair: Stephanie O. Sparks (Hoge Fenton Jones & Appel)

Project Leader: Diane Fiddle (Chief Legal and Privacy Officer, CIPP-US)

INTA Liaisons, Lori Schulman, Erica Vaccarello

AUTHORS AND ACKNOWLEDGEMENTS TO:

Diane Fiddle, (Chief Legal and Privacy Officer, CIPP-US)

Martin Boden, LL.M., IP and Copyright specialist lawyer, Data Protection Officer and Auditor, Owner, Boden Rechtsanwälte (DPC)

Robert Lister, Senior Associate, Data, Privacy and Cybersecurity, Ropes & Gray

Chris Oldknow, EMEA Public Policy, Amazon (DPC)

July 2023

The Digital Services Act, Countdown to Compliance: What Do Brands Need to Know and Do?

The Digital Services Act[1] (DSA) is a signature European Union regulation that introduces new obligations for online intermediary-services providers in all sectors of the economy, primarily to address issues relating to the proliferation of illegal content (including goods and services) disseminated online.

The DSA seeks to regulate digital intermediary services in the EU, as well as those outside the EU that have a significant connection to the EU through targeting or substantial use by EU users.[2] The DSA aims to regulate the internet more strictly and uniformly, thereby creating a safe, predictable, and trustworthy online environment. One of its primary objectives is to protect and guarantee the fundamental rights of internet users and businesses.[3] The DSA also largely preserves and clarifies the limited liability regime under Directive 2000/31/EC (also known as the e-Commerce Directive) and imposes a new set of compliance obligations on intermediary-services providers.

Brand owners, customers, and suppliers all use intermediary services that the DSA will regulate, and they will likely benefit from the new rules. Equally, many brands operate one or more of these intermediary services and will need to take proactive steps to comply with each of the obligations in the DSA applicable to each such service. Users of the services, whether businesses or individual consumers, government or non-governmental organizations ("NGOs"), will see the impact of the DSA on regulated services potentially as early as 25 August 2023 for larger services providers, and from 17 February 2024 for all other service providers.[4] Operators of the services must comply by those dates, and EU Member States must amend any conflicting laws, and designate and set up national regulators by the 17 February 2024 deadline.

Although arguably not as broad in scope and application as certain other EU laws, such as the GDPR,[5] almost every member of the IP Community will need to understand what they must do and what users of intermediary services should expect under the DSA, particularly because fines under the DSA can exceed those under the GDPR. Accordingly, this Paper provides: (1) a high-level overview of the legislative and contextual background of the DSA; (2) the key obligations under the DSA and when they apply; and (3) commentary on the related benefits of the DSA and issues of which members of the IP community should be aware.

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065&qid=1666857835014

[2] See Articles 2(1), 3(d) and 3(e) of the DSA.

[3] See Recital 3 of the DSA.

[4] While all regulated service providers must comply with the DSA by February 17, 2024, all online platforms and online search engines were required to publish their monthly EU user numbers by February 17, 2023. Between then and May 2023, the European Commission plans to designate as "Very Large Online Platforms" or "Very Large Online Search Engines" those platforms and search engines, respectively, with more than 10% of the EU population as active users. If so designated, the relevant service providers must comply with the DSA within four months of their designation by the European Commission. This means that they may need to ensure compliance with the DSA by July 2023 at the earliest and September 2023 at the latest.

[5] GDPR https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

BACKGROUND Legislative development

Following the announcement by the President of the European Commission, Ursula von der Leyen, that the DSA was one of her key political priorities to help shape Europe's digital future, the first draft of the DSA was proposed by the European Commission on December 15, 2020. The European Commission's draft considered over 3,000 responses from stakeholders during a 14-week consultation (including from intermediary-services providers, users of digital services, civil society organizations, academia, and the general public).

Political agreement between the European Parliament and the Council of the EU was reached on April 23, 2022, with the European Parliament formally adopting the DSA in July 2022. The DSA was then published in the Official Journal on October 27, 2022, and came into force on November 16, 2022. Although all obligations under the DSA will apply from February 17, 2024, certain types of intermediary-services providers must comply with specific obligations before that date.

What is the DSA intended to achieve?

As with other landmark EU legislation, such as the GDPR, the European Commission has identified that legislative developments should be on track with rapid advances in technology. Since the e-Commerce Directive was introduced in 2000, the nature, scale, ubiquity, and importance of online intermediary services has changed dramatically and such services are now used on a daily basis by the majority of the EU population—in certain cases, such services have become a key part of the backbone to the digital economy, and some may almost be viewed as "public" online spaces.

The prolific development of online intermediary services across the globe has resulted in significant benefits for society, consumers and businesses alike (such as innovation for consumers and increased efficiency, cross-border trading, and other economic benefits). The European legislators' core concern regarding these developments is that they also facilitate the trade and spread of illegal content (including illegal goods and services) online and the proliferation of harmful practices, such as "dark patterns."[6] The misuse or manipulation of algorithmic systems can further exacerbate this spread, as well as the spread of other harmful content and disinformation.

While the DSA does not define what is illegal online, Ursula von der Leyen has been clear, stating that the DSA "gives practical effect to the principle that what is illegal offline, should be illegal online."[7] Thus, the DSA defines "illegal content" by reference to EU law and EU Member State law (enacted in accordance with EU law).[8] As a result, illegal content will range from dangerous/counterfeit goods, IP-infringing content, and illegal medicines through to cyber bullying/violence and the dissemination of illegal hate speech, terrorist content, and child sexual abuse materials. However, differences could foreseeably arise as to what is or is not illegal depending on the relevant Member State. Illegal content is broadly defined and is not

[6] According to Recital 67 of the DSA, "dark patterns" are practices on online interfaces of online platforms "that materially distort or impair, either on purpose or in effect, the ability of recipients of the service to make autonomous and informed choices or decisions."

[7] https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2545

[8] Article 3(h) of the DSA defines "illegal content" as "any information that, in itself or in relation to an activity, including the sale of products or the provision of services, is not in compliance with Union law or the law of any Member State which is in compliance with Union law, irrespective of the precise subject matter or nature of that law."

just the most serious types of illegal content. A technical breach of a law, such as minor labelling errors on product packaging, would also be covered.

Although some EU Member States had begun legislating in this area (and the e-Commerce Directive already provides for a basic framework regulating the provision of digital services across the EU), the legislation has not been able to keep pace with technological developments, and differing obligations between EU Member States has resulted in a patchwork of distinct regimes that have been interpreted and enforced inconsistently, thereby creating significant barriers to entry, increased compliance costs (particularly for SMEs), and differing standards of protection.

According to the European Commission, the DSA aims to achieve, *inter alia*, the following:

1. **Better protection of EU citizens' fundamental rights online and less exposure to illegal content** (and related harms), through the creation of a fairer, safer and more open, transparent, and accountable online digital space. For society as a whole, the DSA intends to provide greater democratic control and oversight over systemic platforms and mitigate related risks (such as risks posed by illegal content and disinformation).

2. **Harmonize the fragmented rules applicable to (and related liability and enforcement against) intermediary-services providers,** and thereby provide increased legal certainty for such service providers and their users—instead of them having to comply with 27 different sets of EU Member State legislation, such providers will only have to comply with one law, to be interpreted and enforced consistently across the whole EU, which the European Commission believes will ultimately reduce the compliance burden and associated costs. Given that the obligations in the DSA apply asymmetrically (with their application depending on the role, size, and related impact on the online environment of the relevant service provider and small and micro-enterprises generally being exempt from more costly obligations), the DSA is also intended to lower the barriers of entry and compliance costs for new intermediary-services providers, and promote start-ups and scale-ups (and thereby foster innovation, growth and competitiveness both within and outside the EU). For business users of intermediary services, this means greater choice of service providers (and potentially at lower prices); access to EU-wide markets; and greater, more streamlined, transparent, and consistently applied avenues of redress against providers of illegal content hosted on online intermediary services (if their content is unjustifiably moderated or removed from online intermediary services).

3. **Ensure the existing liability (and non-monitoring) regime for online intermediary-services providers remains in place and is harmonized across the EU** (which the European Commission considers to be "a cornerstone of internet regulation"). This means that subject to certain exceptions, intermediary-services providers are not liable for the content provided by their users and are not required to undertake monitoring of user content to determine its legality. The main exception is that hosting providers and online platforms can be held liable in circumstances where they have actual knowledge of illegal activities or are notified that certain content is illegal (in which case they are deemed to have actual knowledge) and do not remove the illegal content.

Although the focus of the DSA is on tackling issues related to the illegal content online, the DSA will also regulate and implement requirements in the fight against the sale of counterfeit

goods as well as other practices considered to be harmful. This includes a ban on use of “dark patterns” by online platforms (i.e., on the basis that these can deceive consumers or otherwise impair or distort their autonomy and choices). Such practices would already be illegal under the Unfair Commercial Practices Directive and may be unlawful under the GDPR.

Further, as explained below, the DSA provides new “Know Your Business Customer” (KYBC) rules to trace sellers on online marketplaces, together with obligations to vet sellers and ensure products offered on their platforms are not illegal. The DSA also imposes transparency requirements about the technology used to support the sale and recommendation of products for purchase to consumers.

As detailed below, users will have new rights, including upgraded mechanisms (with access to dispute resolution capabilities) and expedited channels to detect, report, and remove illegal content through “trusted flaggers.” Users will also have the ability to contest the decisions made by online platforms when their content is removed (e.g., as a seller of goods or publisher of content) and online platforms are obliged to notify them of any decision taken and provide them with access to an effective internal complaints-handling system, through which they are able contest the decision.

Very large online platforms and search engines will be subject to risk assessment obligations (that will require analysis of vulnerabilities to illegal content and harmful practices) and annual audits. There will also be clearer consequences for intermediary-services providers—users will be able to seek damages from providers of intermediary services for infringement of the DSA. The brand protection problems that exist today may be diminished through the implementation of this consumer (and user) protection-focused legislation.

Furthermore, there are DSA obligations relating to online advertising and profiling (due to the importance and prevalence of advertising on online platforms, particularly where advertising revenues play a key role in funding the platform), which also have implications for related direct-marketing and data-protection legislation in the EU (such as Member State laws implementing the e-Privacy Directive and the GDPR). These are explained in further detail below. This focus on the prohibition of targeted advertising and profiling is high on the radar of legislation around the world, as we are increasingly seeing high-profile fines imposed in the Adtech space for GDPR violations related to a lack of transparency in online advertising. Other jurisdictions also have a similar focus. For example, in the United States, following the California Consumer Privacy Act (CCPA) implementation, there has been notable enforcement action taken for targeted ads and failure to honour opt-out requests via browser privacy controls. While this focus on transparent advertising appears to be a tack-on to the DSA, its inclusion illustrates the importance of transparency in advertising and privacy controls to regulators and legislators globally. It is therefore essential for brand owners to have transparent privacy notices, appropriate consent management procedures, clear cookie notices, and a full understanding of how and to whom they market goods and services.

Which services are regulated?

The DSA applies to a wide range of online "intermediary services" that process information provided by their service recipients (whether individual or business users) and that fall under the existing e-Commerce Directive, namely:

- **Mere conduit service providers—**Broadly, this includes providers whose services consist solely of the transmission in a communications network of information provided by the service recipient or the provision of access to such a network (including ISPs

and direct messaging, VoIP, Internet exchange point, VPN, DNS, and domain name registry services);

- **Caching service providers—**Caching services are similar to mere conduit services, except that the services involve the automatic, intermediate, and temporary storage of the information provided by the service recipient, performed for the sole purpose of making the onward transmission of the information more efficient to others upon their request (including content delivery/distribution networks, content adaptation, and reverse proxy services); and

- **Hosting service providers—**These are providers whose services consist of the storage of information provided by, and at the request of, the service recipient (such as cloud and web-hosting services), as well as services that enable the sharing of information or content online (including social media, online marketplaces, and referencing services).

Limited obligations apply to mere conduit and caching service providers under the DSA. In particular, these include obligations to respond to orders to remove illegal content, to provide information in response to orders regarding specific service recipients, to designate points of contact for EU and Member State authorities and recipients of the service, as well as certain new transparency requirements in relation to their terms and conditions and annual reporting. Hosting service providers must comply with additional obligations, including the requirement to implement a notice and action mechanism (to enable any person to submit notifications of the presence of any illegal content and to process those notices), to provide a detailed statement of reasons to affected service recipients (i.e,those whose content is removed on the basis of illegality or non-compliance with applicable terms and conditions), and to inform law enforcement/judicial authorities in the relevant Member State if it becomes aware of any information giving rise to a suspicion of a criminal offense involving the threat to someone's life or safety.

The DSA also supplements the e-Commerce Directive and introduces the following four new categories of services: ***online platforms*** (**OPs**), ***online trading platforms***[9] (i.e., OPs that allow consumers to conclude contracts remotely (distance contracts) with traders of goods or services) (**OTPs**), ***very large online platforms*** (**VLOPs**), and ***very large online search engines*** (**VLOSEs**), to whom additional obligations apply cumulatively. This means that OPs must comply with all obligations applicable to mere conduit, caching, and hosting-services providers, as well as certain specific obligations imposed on OPs. Additional obligations then apply to OTPs, and VLOPs must comply with the largest number of obligations. To the extent that an online service falls into more than one category, then the relevant intermediary-services provider will be required to comply with each obligation applicable to each part of its service.

OPs are a subset of hosting services that not only store information at the request of the recipient of the service, but also make it available to the public (to a potentially unlimited number of third parties) at their request (except, subject to certain limitations, where disseminating the information is a minor and purely ancillary feature of another service or a minor function of the principal service[10]). Examples of OPs include online marketplaces; app stores; and collaborative economy, social media, news/media/content sharing, rating, and

[9] These are referred to in the DSA as "providers of online platforms allowing consumers to conclude distance contracts with traders."

[10] See Recital 13 and Article 3(i) of the DSA.

review platforms. OTPs are a subset of OPs that allow consumers to purchase goods or services from third-party traders online (allowing consumers to conclude distance contracts with third parties who are acting in the course of their trade, business, craft, or profession). This therefore excludes aspects of OP services that allow individuals to sell goods to or buy goods from other individuals, provided the seller is not acting in a business or commercial context. Examples of OTPs include online/e-commerce marketplaces, app stores, collaborative economy platforms, ride-hailing services, and online travel and accommodation platforms.

Exemptions to the supplemental obligations on OPs and OTPs are provided to those OPs and OTPs that qualify as "micro" or "small" enterprises,[11] in order to reduce their compliance burden and related costs, unless they also qualify as a VLOP (though the European Commission has been keen to highlight that micro/small OPs and OTPs can still voluntarily comply with the relevant obligations). To further support scale-ups, if the OP's or OTP's status changes such that they no longer qualify as a micro or small enterprise, they are provided with an additional 12-month grace period before their additional obligations apply (again, except to the extent they qualify as a VLOP).

VLOPs are those OPs with 45 million or more monthly active recipients of the service in the EU (referred to as "active users"), which reflected approximately 10% of the EU population in 2020. Although Recital 28 to the DSA confirms that online search engines are online intermediary services, the DSA does not define a category (mere conduit, caching, or hosting service) for online search engines (something a last-minute amendment during interinstitutional negotiations had sought to do). However, the DSA applies to the extent that they are hosting, caching, or performing some other function that brings them within the DSA, and online search engines must still publish average monthly active user numbers and provide them to the relevant Digital Services Coordinators (DSCs) or the European Commission on request. Online search engines with 45 million or more active users have additional obligations, once designated as VLOSEs by the European Commission. Generally, only the most burdensome and costliest obligations in the DSA are intended to apply to VLOPs and VLOSEs—this is due to "systemic risks"[12] which are said to justify increased responsibility in tackling illegal content online. It should also be noted that although the DSA primarily seeks to provide rules in relation to illegal content, the DSA also imposes responsibilities on VLOPs and VLOSEs in relation to content that may not necessarily be illegal but nonetheless causes systemic issues with the capacity to cause harm (including disinformation and manipulation during pandemics or elections).

Finally, it is important to note that the DSA does not seek to regulate digital services that are not intermediary services.[13] As a result, to the extent that website owners or online service providers do not qualify as intermediary-services providers (i.e., where they have responsibility for their own content), such owners and service providers will not be subject to the DSA, even if the relevant service is provided through the use of an intermediary service.[14]

[11] The DSA defines "micro enterprises" and "small enterprises" by reference to Recommendation 2003/361/EC (https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:124:0036:0041:en:PDF). This means that an OP/OTP will qualify as: (a) a micro enterprise if has fewer than 10 employees and its annual turnover and/or annual balance sheet total does not exceed EU 2 million; or (b) as a small enterprise if it has fewer than 50 employees and its annual turnover and/or annual balance sheet total does not exceed EU 10 Million.

[12] For more information on systemic risk see https://cerre.eu/publications/what-is-the-harm-in-size/.

[13] See Recitals 5 and 6 and Articles 2 and 3(g) of the DSA.

[14] See Article 2(2) of the DSA.

WHAT ARE THE NEW OBLIGATIONS?

The obligations in the DSA are layered. Services that are more technical or on an infrastructure level have fewer obligations while those that are considered by legislators to pose the greatest risks (VLOPs) have the greatest number of obligations. Obligations in the DSA are overseen and enforced by either nationally designated regulators known as Digital Services Coordinators (DSCs) (which may be new or existing independent authorities), or the European Commission. The European Commission has exclusive powers to supervise and enforce certain obligations under the DSA that are solely applicable to VLOPs and VLOSEs (although DSCs can enforce other DSA obligations against VLOPs and VLOSEs if the European Commission chooses not initiate proceedings for the same infringement.

The key new obligations in the DSA are set out in **Annex 1**, which provides an overview of all primary obligations and to whom they apply. These include obligations on intermediary-services providers to:

- **Respond to orders** to act against items of illegal content (or for information on particular service recipients) from national judicial/administrative authorities and **inform them of the effect given to the order.**[15]

- **Designate points of contact** for Member State authorities, the European Commission and service recipient, and (if the intermediary-services provider is not established in the EU) **appoint a Legal Representative** in one of the Member States in which the services are offered. Details of the points of contact and (if applicable) Legal Representative must be published publicly. If a Legal Representative is appointed, the intermediary-services provider must notify the name and contact details of the Legal Representative to the DSC of the Member State in which the Legal Representative is located.

- **Provide information in their service Terms and Conditions on any restrictions regarding content provided by service recipients** (including any policies, procedures, measures, and tools used for the purpose of content moderation (such as algorithmic decision-making and human review) and the rules of procedure for complaints.[16] This provision aims to ensure greater transparency in the handling of content and data provided by users. Intermediary-services providers must then also **act in a diligent, objective, and proportionate manner when applying such service restrictions** (including with due regard to the rights and legitimate interests of all parties involved). This means, for example, that intermediary-services providers must take into account the fundamental rights of service recipients (such as the freedom of expression, and freedom and pluralism of the media) when applying their service Terms and Conditions.

- **Publish annual transparency reports on their content moderation activities**, including (subject to certain categorization requirements) the number of orders received from national judicial/administrative authorities, the median time taken to respond and give effect to those orders, information about content moderation

[15] See Articles 9 and 10 of the DSA.

[16] See Article 14 of the DSA.

activities taken at the service provider's own initiative, the number of complaints received, and the use of automated means for content moderation.[17]

- **Implement a specific form of electronic notice and takedown process,[18]provide a detailed statement of reasons to affected service recipients[19] and report serious (life or safety-threatening) criminal offenses to authorities.**[20] Specifically, and importantly, for brand owners, providers of hosting services must implement mechanisms to allow any individual or entity to notify the hosting provider of the presence of any content on their service considered to be illegal (and certain related information, such as why the content is considered to be illegal and where the content is located). The provider must, without undue delay, inform the complainant about its decision and the possibilities for redress. In some Member States (such as Germany with the NetzDG (Network Enforcement Act)), such notice and takedown procedures are already provided to users of social media platforms. New is the right to contest the decision, which will make it necessary for intermediary-services providers to implement transparent and effective procedures to ensure access to an internal complaint-handling mechanism, out-of-court dispute settlement, and judicial redress.

  In circumstances where the service provider decides to remove allegedly illegal content or limit access to content (or take other similar actions, such as demoting or demonetizing content, or suspending or terminating service or account access), it must inform the affected service recipients with a clear and specific statement of the reasons. That statement of reasons must contain certain, specific information.[21] OPs will also be required to submit anonymized versions of each decision and statement of reasons to the European Commission without undue delay.[22] This information will then be made publicly available in a machine-readable database managed by the European Commission. The expectation is that this increased transparency will reduce the number of arbitrary decisions taken by OPs; if user accounts are deactivated or content is removed by reference to the service Terms and Conditions, OPs will need to clearly

[17] See Article 15 of the DSA. Note that VLOPs and VLOSEs must publish their transparency reports at least every six months following their designation by the European Commission. Hosting providers are required to include additional information in their transparency reports, such as: (i) the number of notices submitted alleging the presence of illegal content on their service, categorized by the type of alleged illegal content; (ii) the number of notices submitted by Trusted laggers; (iii) any action taken, distinguishing between actions taken on the basis of illegality or infringement of service Terms and Conditions; (iv) the number of notices processed by automated means; and (v) the median time to take action in response. VLOPS are also subject to enhanced transparency reporting rules under Article 42 of the DSA.

[18] This obligation does not apply to mere conduits and caching services providers, pursuant to-services provider of the presence of illegal content on their service.

[19] See Article 17 of the DSA.

[20] See Article 18 of the DSA.

[21] Pursuant to Article 17 of the DSA, the statement of reasons must include certain mandatory information, including: (i) what the decision entails and its territorial scope; (ii) the facts and circumstances relied on in taking the decision; (iii) information on any automated means used in making the decision; (iv) if the decision relates to allegedly illegal content, an explanation as to why the content is considered to be illegal; (v) if the decision is based on infringement of the service Terms and Conditions, a reference to the contractual ground relied on and an explanation as to why the content infringes that ground; and (vi) the possibilities for redress regarding the decision, where applicable, through internal complaint-handling mechanisms, out-of-court dispute settlement and judicial redress.

[22] See Article 24 of the DSA.

articulate why and must take into account the rights of the affected service recipients.

- **Provide access to an effective internal complaints-handling system for content moderation/removal decisions and suspend service provision to service recipients (or their accounts) in certain circumstances.**[23] The complaints-handling system must be easily accessible and user-friendly and must enable service recipients to lodge complaints free of charge against decisions taken by OPs. OPs must also handle complaints in a timely, non-discriminatory, diligent, and non-arbitrary manner, reverse decisions in certain circumstances,[24] and inform complainants without undue delay of their decision (together with the possibility of out-of-court dispute settlement and other available possibilities for redress). This requirement is intended to prevent platforms from operating without appropriate complaints-handling mechanisms, as well as ensure that service recipients' fundamental rights are respected.

  Under Article 21 of the DSA, service recipients whose complaints are not resolved through the intermediary-services provider's internal system are entitled to have the issue referred to any out-of-court dispute settlement body that has been certified by a DSC. OPs must ensure that information about this right is clearly presented on their online interfaces and must also engage in good faith with the settlement body selected, with a view to settling the issue. Although the settlement body will not have the power to impose a binding settlement on the parties, the OP must pay all fees charged by the settlement body and reimburse the service recipient's reasonable expenses if the dispute is decided in favor of the service recipient. If the OP wins the case, it still bears its own costs (except where the settlement body determines that the service recipient manifestly acted in bad faith). Avoiding these further costs may further motivate OPs to ensure that their decisions respect the rights of all interested parties or that complaints are resolved through their internal systems.

  However, platforms will not be powerless. If certain service recipients frequently file manifestly unfounded complaints, then—after issuing a warning—OPs must suspend (for a reasonable period of time) the processing of complaints from those service recipients.[25] In addition, OPs will not be required to engage with the settlement body in respect of disputes that have already been resolved (i.e., regarding the same information and grounds).[26] It remains to be seen whether this limited provision will be sufficient to address misuse of the very specific processes that the DSA requires.

- **Implement technical and organizational measures to ensure takedown notices from "Trusted Flaggers" are prioritized, processed, and decided without undue**

[23] These obligations only apply to OPs pursuant to Articles 20 and 23 of the DSA. Micro and small enterprises are exempt from these requirements, unless they also qualify as a VLOP.

[24] Under Article 20 of the DSA, decisions must be reversed without undue delay where the complaint contains sufficient grounds for the OP to consider that: (i) its decision not to take action on the notice is unfounded; (ii) the content is not illegal and/or is not incompatible with the service Terms and Conditions; or (iii) the complaint otherwise substantiates that that the complainant's conduct does not warrant the measure(s) taken.

[25] See Article 20(2) of the DSA. The same principle also applies in respect of service recipients that frequently file manifestly unfounded takedown notices.

[26] See Article 21(2) of the DSA.

delay.[27] The status of a Trusted Flagger can only be awarded on application to and by DSCs to those entities[28] that have demonstrated all of the following qualifications:

- particular expertise and competence in detecting, identifying, and notifying illegal content;
- independence from any online platform; and
- carries out its activities for the purpose of submitting notices in a timely, diligent, and objective manner.

In particular, industry associations representing their members' interests are encouraged to apply for the status of Trusted Flaggers.[29] Intellectual property rights organizations, industry associations and even individual right-holders could be awarded Trusted Flagger status if they meet the criteria, although the overall number of Trusted Flaggers is to be limited.

- **Ensure certain KYBC information is obtained, in advance, before allowing traders to promote messages or offer products or services to EU consumers on the relevant platform**, **make best efforts to assess whether the information is reliable and complete** (before allowing the trader to use the services), and **suspend service provision to traders** (in relation to the offering of goods/services to EU consumers) **if inaccurate, incomplete, or out of date information is not corrected or completed without undue delay**.[30] These requirements mark some of the most significant provisions for brand owners. OTPs must obtain and verify certain basic information before allowing traders to sell on their platform, including each trader's name and contact details, its trade register number and the trade register (if applicable), and a self-certification by the trader committing to offer only products or services that comply with the applicable rules of EU law. This basic information must be easily accessible to the public and at least available where the trader's goods or services are presented on the OTP's interface. Other information, such as each trader's electronic identification information and its payment account details must also be collected and verified, but may only be disclosed when necessary under applicable law (e.g., pursuant to an order from national judicial/administrative authorities). OTPs must design and organize their online interfaces in a way that enables traders to comply with their obligations regarding pre-contractual and product safety information. While OTPs are required to use best efforts to ensure the information provided is reliable and complete, Recital 73 of the DSA states clearly that OTPs should not be required to engage in excessive or costly (online or offline) fact-finding exercises to determine the accuracy of the information provided. Accordingly, where OTPs can demonstrate that they have used their best efforts, OTPs will not be held as guaranteeing the reliability of the information provided to consumers or other interested parties. The traders themselves remain liable for the accuracy of the information they submit to the OTPs.

[27] This obligation only applies to OPs pursuant to Article 22 of the DSA. Micro and small enterprises are exempt from this requirement, unless they also qualify as a VLOP.

[28] Recital 61 to the DSA clarifies that Trusted Flagger status will not be awarded to individuals.

[29] See Recital 61 of the DSA.

[30] This obligation only applies to OTPs, pursuant to Article 30 of the DSA. Micro and small enterprises are exempt from these requirements, unless they also qualify as a VLOP.

- **Very large online platforms have a variety of requirements including frequent transparency reporting**, with oversight by the EC rather than purely by a Member State, risk assessment,[31] risk mitigation,[32] being subject to independent audit,[33] the necessity of providing a non-personalized option for recommender systems,[34] the need to create a public repository of advertising,[35] and being subject to data access by vetted researchers.[36] These are some of the most onerous provisions of the DSA and the ones for which more guidance is likely after February 2024, once the Board of the DSA Member State regulators is in place. At launch, they will only apply to around 20 services, but any service wanting to cover the single market or even a few of the largest Member States is likely to reach the threshold quite quickly and will need to plan for the moment when these obligations apply to them as this is a big "asymmetric" lift that risks becoming a glass ceiling. For the smallest micro-services, there is a 12-month transition to compliance with the main rules that is not mirrored for the transition to becoming a VLOP or VLOSE.

Online advertising obligations under the DSA

As highlighted above, OPs will also need to comply with certain new obligations regarding online advertising (whether traditional business-to-consumer advertising or issue-based or political advertising) and profiling. According to the Recitals to the DSA, online advertising has the capacity to contribute to risks in relation to illegal and harmful content and activities (including where the advertisements themselves constitute illegal content) and discriminatory advertising practices can impact equality.[37] The new rules should also assist service recipients to better understand the advertisements they see and to make more informed decisions in that regard (e.g., to reject cookies used for such purposes or to object to the use of their personal data in this way).

In particular, OPs must:

- **Provide functionality to service recipients to declare whether the content they provide is (or contains) commercial communications**,[38] including, for example, sponsored content or commercial messages promoted by influencers, and **ensure that those who access that content can identify its commercial nature in a clear and unambiguous manner**.

- **Ensure that each individual recipient of each advertisement presented on the OP's platform is able to identify (in a clear, concise, and unambiguous manner, and in real time) certain transparency information about such advertising**.[39]

  This information includes:

[31] See Article 34 of the DSA.

[32] See Article 35 of the DSA.

[33] See Article 37 of the DSA.

[34] See Art. 38 of the DSA and page paragraph 2 of this Paper.

[35] See Art. 39 of the DSA and pages 11 and 12 of this Paper.

[36] See Art. 40 of the DSA and pages 13-14 of this Paper.

[37] See Recital 68 of the DSA.

[38] See Article 26 of the DSA. Micro and small enterprises are exempt from this requirement, unless they also qualify as a VLOP.

[39] See Article 26 of the DSA. Micro and small enterprises are exempt from this requirement, unless they also qualify as a VLOP.

- whether the relevant information is an advertisement;
- the person/company that is presenting the advertisement;
- if different, the person/company that paid for the advertisement; and
- meaningful information (directly and easily accessible from the advertisement) on the main parameters and logic used to determine the recipients of the advertisement (including whether this is based on profiling) and, where applicable, how to change such parameters.

The DSA will therefore require OPs to be much clearer about how advertisements are presented, and if contextual or targeted advertising (or any related profiling) is used, the related criteria and how to change those criteria. This is likely to be straightforward in the case of contextual advertising, but for targeted advertising, the new obligations will require significantly more transparency. This means that OPs and advertising brand owners will be forced to disclose more detailed information about how and why recipients are chosen to receive the respective advertisements, e.g., for their age, gender, or interests. This form of transparency is likely to lead to more complaints and objections by recipients and impede certain established advertising models. Brand owners should carefully consider whether they really want to make use of targeted ads, since the disclosure of the targeting method and the collected data will become clearer to the wider public, data protection regulators, and supervisory authorities.

At the same time, this all still needs to be conducted in accordance with the GDPR and Member State laws implementing the ePrivacy Directive, in particular obligations regarding the right to object, automated individual decision-making (including profiling), and the need to obtain consent of the data subject prior to the processing of personal data for direct marketing purposes, such as targeted advertising.

Article 39 of the DSA also imposes additional obligations on VLOPs and VLOSEs regarding advertisements presented on their online interfaces. In particular, VLOPs and VLOSEs will be required to compile and publish a repository[40] containing certain information about the advertisements presented. This includes information about: the content of each advertisement (such as the name of the brand and subject matter of the advertisement); the person on whose behalf the advertisement is presented (and, if different, who paid for the advertisement); the period during which the advertisement was presented; whether the advertisement was intended to be displayed to one or more particular groups of service recipients of the service, and, if so, the main parameters used for that purpose; the total number of service recipients of the service reached; and, where applicable, aggregate numbers for the group or groups of recipients to whom the advertisement was targeted. However, although Article 39 requires that the repository must not contain any personal data relating to service recipients that were presented with the relevant advertisements, there appears to be no protection for the personal data of individuals as advertisers in these disclosures; this may be addressed in additional guidance from the European Commission or European Board for Digital Services (EBDS).

- **Provide certain details in the service Terms and Conditions regarding their use of any "recommender systems"**[41] and, where there are several options available to

[40] The repository must be publicly available in a specific section of the VLOP's or VLOSE's online interface, through "a searchable and reliable tool allowing for multicriteria queries and through APIs."

[41] Article 3(s) of the DSA defines a "recommender system" as "a fully or partially automated system used by an online platform to suggest in its online interface specific information to recipients of the service or prioritise that

determine the order of the content presented, **make available functionality for service recipients to select and modify their preferred option**.[42] OPs will be required to clearly describe the main parameters used in their recommender systems (including the most significant criteria in determining the information suggested and the relative importance of those parameters) and what options are available to modify or influence those parameters. In addition, VLOPs and VLOSEs will need to ensure that at least one option is not based on profiling.[43] This may make some services considerably less user friendly and, where based on targeted advertising, could lead to a disruption in the revenue models for VLOPs and VLOSEs. For brand owners, this change necessitates a rethink of how to present products, when targeting is not desired or possible.

- **Ensure[44] service recipients are not presented with advertisements based on profiling**[45] **using special categories of personal data.**[46] The rationale for this prohibition is that targeted advertising using such sensitive personal data may have damaging effects and "manipulative techniques can negatively impact entire groups and amplify societal harms, for example by contributing to disinformation campaigns or by discriminating against certain groups."[47]

  Although the DSA is not intended to modify the GDPR, this ultimately seems to be the practical effect. The GDPR contains no such prohibition on targeted advertising, and while likely very difficult to achieve in practice, the processing of special categories of personal data in this way could conceivably be carried out lawfully and in accordance with the GDPR (on the basis of a GDPR-compliant explicit consent or where the relevant personal data had otherwise been made public by the service recipient as a data subject). The European Data Protection Board has also explored this issue previously in the context of its Guidelines on targeting of social media users.[48] Although these Guidelines highlight certain difficulties in ensuring compliance with the GDPR in this regard (in particular that the OP and advertiser will be joint controllers in such circumstances and that it will likely be tricky to establish an appropriate legal basis

information, including as a result of a search initiated by the recipient of the service or otherwise determining the relative order or prominence of information displayed."

[42] See Article 27 of the DSA. Micro and small enterprises are exempt from these requirements, unless they also qualify as a VLOP. Under Article 40 of the DSA, VLOPs and VLOSEs will also be required, on request, to explain the design, logic, functioning and testing of the algorithmic systems they use (including any recommender systems).

[43] See Article 38 of the DSA.

[44] See Article 26 of the DSA. Micro and small enterprises are exempt from this requirement, unless they also qualify as a VLOP.

[45] Article 4(4) of the GDPR defines this as "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements."

[46] "Special categories of personal data" refers to, as per Article 9(1) of the GDPR, personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

[47] See Recital 69 of the DSA.

[48] See https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_082020_on_the_targeting_of_social_media_users_en.pdf

under Article 9 of the GDPR), it stops short of stating this is impossible or otherwise unlawful.

- **Implement appropriate and proportionate measures to ensure a high level of privacy, safety, and security for minors** using their service, and **ensure minors are not presented with advertising based on the profiling of their personal data.**[49] This is going to be a difficult and onerous obligation for any OP whose service is accessible to minors (including where the OP's Terms and Conditions permit access by minors, where the service is directed at or predominantly used by minors, or where the OP is otherwise aware that some users are minors). For example, when setting targeting cookies, in many cases it is going to be very difficult for OPs to know whether the service recipient is a minor. However, this ban on targeted advertising to minors will only apply where the OP is aware (with reasonable certainty) that the recipient of the service is a minor and Article 28(3) of the DSA clarifies that this obligation does not require OPs to process additional personal data about its service recipients to assess whether they are minors. This may ultimately provide some comfort to OPs in this regard. At best, this may also lead to a significant reduction in the (often) arbitrary use of cookies by OPs.

For IP lawyers, the potential access to VLOP data by vetted researchers should be a focus, given the narrow safeguards for trade secrets and IP protection in the DSA.[50] For Data Protection lawyers, this new law should be reviewed for its additional accountability and transparency measures regarding the processing of service recipient data, including the ban on targeted advertising using special characteristics of service recipients or, more broadly, to any minors. The data processed by OPs and online search engines is largely that of the service recipients, as providers or consumers of the service based on interactions when using the platform. This data is largely personal or commercially confidential to individual or business users. In giving researcher access, the risks from loss of this data through accident or through targeted cyber-attack on the researcher, are and will continue to be significant. For example, what if a vetted researcher's project on whether searches for counterfeit goods creates or poses a future systemic risk is approved by the home DSC of a VLOSE? The VLOSE is then required to make the search results relevant to the project available to the researcher. This is a potentially very large data set of personal searches by EU citizens. A data breach involving this data would be very serious. Alternatively, this could be research involving datasets of sales of healthcare brands on VLOP marketplaces involving direct sales by brands as well as authorized and unauthorized sellers. This could be commercially sensitive to each of these groups. Both data sets would be very attractive to hackers for both commercial and political use by both non-state and state actors. Considerable technical and human protections, e.g., data vaults,[51] would be needed to secure the data to manage its handling for the whole period this was available outside the VLOP or VLOSE. However, DSCs are required to terminate a vetted researcher's access to the data if they are no longer capable of fulfilling their specific data security and confidentiality requirements corresponding to their research request or to otherwise protect personal data appropriately.

[49] See Article 28 of the DSA. Micro and small enterprises are exempt from these requirements, unless they also qualify as a VLOP.

[50] See Article 40 and Recitals 97 and 98 of the DSA. A delegated act setting out more of the specifics of the procedures is expected in the first half of 2024.

[51] See recital 97 of the DSA.

TIMELINE FOR IMPLEMENTATION OF THE DSA

Stage 1: February 17, 2023—What happened: Counting your users

The DSA first required, by 17 February, 2023 (and at least once every six months thereafter), for OPs and online search engines to publish, for each platform and online search engine they operate, information about their average number of active monthly EU service recipients over the previous six months, in a publicly available section of their online interface.[52] This information will then be used by the European Commission, to determine and designate VLOP and VLOSE status, respectively, under Article 33 of the DSA.

OPs and online search engines only need to count unique[53] and active[54] EU service recipients (including both individual and business users) and are permitted to discount visits by bots and scrapers (where their technology allows) or duplicate user visits, such as when a particular service recipient accesses the service by mobile app and then through a web browser at home or at work. The DSA is clear that service recipients do not need to be logged in when using the relevant service, so OPs and online search engines need to count all unique visits where clicking or scrolling or searching occur. The Commission published a Q&A[55] that provides further information regarding the reporting obligations under Article 24 of the DSA. The Q&A also clarifies that OPs need to count third party traders and advertisers in the EU using their platform and that consumers do not need to purchase goods or services on an OTP marketplace to be counted.

Although the DSA does not require OPs and online search engines to perform any particular tracking of service recipients, how a service can identify each of those attributes in order to calculate its average EU service recipient numbers accurately and effectively will clearly require certain data collection; if that includes the collecting and processing of personal data, then this must still be performed in accordance with the GDPR. However, the Q&A highlights that the DSA neither requires nor permits OPs or online search engines to conduct profiling or tracking of service recipients to avoid double counting. Accordingly, it seems unlikely that OPs and online search engines will be able to assert that such processing is necessary for compliance with a legal obligation as their legal basis under Article 6 of the GDPR in such circumstances.

The outcome of this exercise has been a frustrating first stage in the implementation process that has hinted at some of the problems from rushed legislation that will need ironing out through formal guidance and early communication from regulators. In particular, there has been, to date, a very low number of platforms that have appeared to comply with this reporting obligation (or otherwise complied in ways that the European Commission had not expected).

---

[52] See Article 24(2) of the DSA. Micro and small enterprises are exempt from this requirement, unless they also qualify as a VLOP. However, micro and small enterprises are still required to comply with the requirements of Article 24(3) of the DSA, which requires all OPs and online search engines to communicate without undue delay to their home DSC or the European, on request, information about on their active EU service recipients at the time of the request, together with any other information regarding their related calculations.

[53] See Recital 77 of the DSA. Recital 77 of the DSA also clarifies that all unique, active service recipients need to be counted, not just (where relevant) registered users.

[54] See Articles 3(p) and 3(q) of the DSA. Under Article 3(p) of the DSA, an "active recipient of an online platform" is defined as a service recipient that has engaged with an OP by either: (i) requesting the OP to host information; or (ii) being exposed to information hosted by the OP and disseminated through the OP's online interface. Under 3(q) of the DSA, an "active recipient of an online search engine" is defined as a service recipient that has: (i) submitted a search query to the online search engine; and (ii) has been exposed to information indexed and presented on the online search engine's online interface.

[55] https://digital-strategy.ec.europa.eu/en/library/dsa-guidance-requirement-publish-user-numbers

The European Commission has been unable to provide formal guidance ahead of 2024 because this would require input from DSCs (which have not yet been established), and there has been little time for Member States or the European Commission to mount a broad awareness campaign to businesses. As a result of ambiguity in the text to the DSA and the Q&A, those OPs that did publish information took a variety of approaches, with around half taking a more conservative approach by merely indicating whether they had more or less than 45 million active users. Prior to the publication of formal guidance, many OPs saw a specific but inherently inaccurate number as competitive commercial information. Inevitably, some other OPs reported numbers or information that seems surprisingly low and under the 45 million mark while others pointed out that their total under the methodology would exceed one billion users, over twice the population of the EU. How this issue will develop remains to be seen, though it is conceivable that delegated acts could be adopted requiring more prescriptive information in this regard.

Implementation execution: The EC oversees VLOPs and VLOSEs

There is a new unit of the Directorate-General for Communications Networks, Content and Technology (DG CNECT) that now acts as the EU regulator for the VLOPs and VLOSEs under the DSA.[56] This political compromise was added during DSA negotiations to address Member State frustrations regarding cross-border enforcement of the GDPR, while preserving the country-of-origin standard that allows intermediary-services providers to reach the single market from a single Member State. The composition of the unit in DG CNECT is still not entirely clear. The European Commission has said that a "societal issues" team will oversee the risk assessment and mitigation obligations, for example.[57] The assessments and mitigation plans will be submitted to DG CNECT and there is a process of independent audit to be completed.[58]

The European Commission has exclusive competence for overseeing and enforcing the additional obligations that apply to VLOPs and VLOSEs under the DSA,[59] while they share competence with the DSCs for the other obligations.[60] Until the home Member State of a VLOP or VLOSE establishes its DSC, or allocates tasks to other competent authorities, only the European Commission will be able to enforce the DSA against VLOPs and VLOSEs.

Brand owners will be able to raise compliance concerns about VLOPs and VLOSEs with the European Commission, starting four months after OPs and online search engines are designated as such by the European Commission, and to DSCs in respect of all other intermediary-services providers as of February 17, 2024. These concerns will need to relate to the processes of the services, not their individual decisions. The DSA aims to regulate

[56] The unit is led by Prabhat Agarwal https://op.europa.eu/en/web/who-is-who/organization/-/organization/CNECT/COM_CRF_244077

[57] https://www.linkedin.com/pulse/sneak-peek-how-commission-enforce-dsa-dma-thierry-breton/?trackingId=tg8vn7Mrg88Kqv3ZlZi1YQ%3D%3D

[58] Articles 34, 35 and 37 of the DSA.

[59] See Article 56 of the DSA.

[60] Under Article 56(4) of the DSA, if the European Commission does not initiate proceedings against a VLOP or VLOSE for the same proceedings (i.e. in respect of obligations that are not exclusive to VLOPs and VLOSEs), then the home DSC of the VLOP or VLOSE will have the power take enforcement action against the relevant VLOP or VLOSE.

processes, not content.[61] The DG CNECT unit will have considerable pressures ahead of February 2024, as it must assess and designate VLOPs and VLOSEs from amongst the 10,000 OPs it estimates exist and establish relationships with them. The European Parliament elections are also planned to take place in May 2024, so another major focus in the first year will be on working with VLOPs and VLOSEs to protect this process from interference that undermines the democratic process, possibly the most fundamental systemic risk.

Stage 2: VLOP and VLOSE designations enforceable within four months

The European Commission designated the first 19 services as VLOPs and VLOSEs on April 25 2023 .[62] The providers must move forward to fulfil the additional obligations applicable to VLOPs and VLOSEs pursuant to Section 5 of Chapter III of the DSA; among them obligations regarding undertaking (systemic) risk assessments, implementing mitigation measures to address the systemic risks identified, complying with any actions required under crisis decisions adopted by the European Commission, and submitting to annual audits, which all become enforceable four months after their designation as VLOPs or VLOSEs.[63] The Commission has said that enforcement would be from August 25, 2023.

Stage 3: Full Implementation of the DSA by February 17, 2024

On February 17, 2024, when the DSA comes into full force, brands will have far wider opportunities to improve their online enforcement, with tens of thousands of intermediary-services providers coming under the oversight of Member State DSCs. By this deadline, intermediary-services providers must have designated points of contact and, if they are established outside the EU, Legal Representatives in the EU. Hosting services providers (including OPs and OTPs) should have put in place processes for handling takedown notices and act on them (although some infrastructure providers may pass on notices to their user-facing clients[64]) and all marketplaces should have implemented KYBC procedures to verify details of professional traders selling goods or services through their platforms.

Brands will have much more information about what services are doing and why. In summary, the actions that will need to be in place are:

- Providers of intermediary services shall provide information on any policies, procedures, measures, and tools used for the purpose of content moderation, including algorithmic decision-making and human review in their Terms and Conditions.
- Providers of intermediary services must report annually on their content moderation activity in response to authority orders, regarding any proactive measures they have taken, including restrictions of service affecting visibility of content, and in the training of staff.
- Hosting providers will provide further data on notices received, breaking out the number from Trusted Flaggers, and the median time for action.

[61] However, an exception to this principle would apply, if hosting providers and platforms do not sufficiently respect the fundamental rights of users when restricting the use of their services. In this case, it would depend on the concrete content of the terms and conditions and not only on their provision.

[62] See https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2413/smo

[63] See Article 92 of the DSA.

[64] See recital 51 of the DSA.

- Online platforms will also report on the internal complaint and ADR processes.
- The EC will host a database of all the statements of reasons in respect of notices, building a large repository of knowledge of what actions are taken and why.

Designation of competent authorities and DSCs

National oversight of intermediary services will clearly be a significant undertaking. By February 17, 2024, EU Member States must have designated one or more competent authorities to be responsible for the supervision of intermediary-services providers and enforcement of the DSA. In addition, Member States must designate one of the competent authorities as their DSC. Establishing a DSC is no small task. A DSC will need expertise to oversee intermediary services of all types across all sectors of the economy. Member States will also need to put in place mechanisms for effectively coordinating with the other regulatory experts, as well as participating in cross border coordination at a Board that DG CNECT needs to consult on various topics[65] and in handling other tasks bilaterally with other DSCs over cross-border orders, for example.

It is not clear yet who will be the regulator in most Member States. Ireland is proposing a media regulator, another Member State is proposing its telecom regulator, while others are considering their privacy, consumer, or competition authorities. Whichever agency is the appointed DSC, the Board of the national DSCs will bring very different regulatory cultures and experiences, which could foreseeably result in inconsistent approaches to enforcement between Member States.

Member States may also need to amend their national laws to align with the DSA. The original draft of the DSA required the European Commission to provide guidance on how to fit the DSA into the framework of existing EU law, but that was removed in the final text. There is much to be done in many Member States, as one of the key drivers for the DSA was the fragmentation of Member State laws on illegal content, most prominently the NetzDG in Germany. Surprisingly, however, the authorities responsible for enforcing the NetzDG will not be appointed as Germany's competent DSC under the DSA (for not providing the level of independence from government required under the DSA). As a result, Germany is currently considering the creation of a totally new, impartial body.

The challenge that Germany faces in this regard is one reason why many Member States are concerned that they will not have time to pass the domestic legislation necessary to amend their laws and to appoint and empower a DSC before February 2024. This may also mean that many Member States will not have DSCs in place by the time that the DSA applies in full to VLOPs and VLOSEs, which will likely mean that the European Commission will be solely responsible for monitoring and enforcing compliance under the DSA until they have done so.

SANCTIONS UNDER THE DSA

The European Commission is exclusively responsible for imposing fines on VLOPs and VLOSEs that do not comply with the additional obligations of the DSA applicable to them.[66] These fines may not exceed six percent of their annual worldwide turnover.[67] New, compared

[65] See recitals 91-149 of the DSA.

[66] See Article 56 Nr. 2, Article 73, Article 74 of the DSA.

[67] Article 74 Nr.1 of the DSA.

to the sanction system of the GDPR, is the possibility of imposing periodic penalty payments if VLOPs and VLOSEs do not comply with decisions of the European Commission, e.g., requests for information or on-site inspections. As soon as the platforms comply with their obligations, the Commission may set the final amount of the periodic penalty at a figure lower than originally set.[68]

For other intermediary-services providers, the same system applies regarding the maximum amount of the fine as well as the possibility for periodic penalty payments. However, it is up to the Member States to lay down their own rules on the penalties to be imposed. These must be effective, proportionate, and dissuasive.[69] The penalties will be imposed by the competent DSC in the relevant Member State.[70] DSCs will also be able take enforcement action against VLOPs and VLOSEs for failure to comply with DSA obligations that do not apply exclusively to them, to the extent that the European Commission decides against undertaking enforcement proceedings against them for the same infringement.[71]

Any service recipient also has the right to lodge a complaint with the competent DSC alleging a failure to comply with DSA obligations by any intermediary-services providers.[72] Similar to Article 82 of the GDPR, service recipients will also benefit from the right to seek, in accordance with EU and Member State law, compensation from intermediary-services providers, in respect of any damage or loss suffered due to an infringement of the DSA by those providers. It is therefore to be expected that committed service recipients may be motivated to identify breaches of the DSA for their own financial benefit.

CONCLUSION

The GDPR took four years of negotiation. The DSA was a sprint through COVID-19 lockdowns and was completed in under 18 months. The DSA provisions come into force in three, eight, and 15 months, far faster than GDPR and equivalent legislation like the Market Surveillance Regulation. It will take time for the DSA to be implemented and understood, and for the unresolved problems to be addressed.

This Paper has set out the issues the DSA looks to address, who it regulates, the tools it provides to brand owners and consumers, and the road to implementation. For brands, the first step is to assess obligations and, if parts of their businesses are regulated, how to ensure compliance. As consumers of services, the second step is for brands to look at what regulated businesses they currently use and whether the DSA motivates the reconsideration of any of those uses. Third, as owners of intellectual property, brands must consider how best to utilize the tools of the DSA to advance brand and content protection with greater speed, lower cost, and better results. In brand enforcement, there will be a huge change in the volume of available information about content moderation and tools to help in the enforcement against counterfeit goods. There will be the ability to request action from services that may have previously ignored requests. For the largest platforms, it will be a balance between ensuring that existing systems continue to operate and are updated so that they are not disrupted by new volumes of notices flooding in from more expansive and diverse sources.

[68] See Article 76 of the DSA.

[69] See Article 52 of the DSA.

[70] See Art. 49, 51 (Nr. 2 c) of the DSA.

[71] See Art. 56 Nr. 4 of the DSA.

[72] See Art. 53 of the DSA.

As discussed above, many of the obligations under the DSA reflect practices already in place by responsible service providers. The new notification process means anyone can send a notice, not just brands or their representatives. That is likely to increase the volume of erroneous or malicious notices being received by the teams that brands usually deal with on a platform.

As explained, a new category of Trusted Flaggers is created by the DSA. Trust Flaggers are a designated source for notice conformity, authenticity, and confirmation. Their notices to online platforms are to be treated with priority. Brands will need to consider whether they or their trade associations want to apply for Trusted Flagger status. Trusted Flaggers are designated by national DSC authorities, but these authorities may not come into existence until February 2024 (or later, given the readiness of several Member States). Trusted Flaggers have transparency obligations so the decisions of whether to apply for this status, in which country, and which categories of illegal content to be responsible for, requires careful consideration, especially as this status only relates to notifying online platforms, not all services.[73]

A significant advancement for brands, brand protection, and enforcement efforts is that platforms will now be required to give reasons for their decision about a notice received regarding a take down regardless of the source of the notice. They must submit the decisions to a database set up by the EC. Their decisions can be challenged through an internal-complaints procedure and again through Alternative Dispute Resolution (ADR). Brands should expect many more of their notices to be challenged by users (*i.e.* any individual or entity). The implementation of the new system will be fluid over time, as the ADR providers are appointed by national DSCs, so they will not be in place until February 2024, and the EC does not intend to have an operational database before that date either.

Brands will find that their advertising on VLOPs and VLOSEs is placed in a publicly accessible repository, along with information about what they spent on the advertising and which agency this was spent through. The details of the main audience targeting criteria will also be public, as will the achieved reach. If this raises concerns about sharing data of your client or business, then you should start thinking now about what you will do before July 2023 to prevent this information from becoming public. For sole traders, they may also be concerned about disclosure of their personal details. The upside to this massive publication, will be the ability of brand enforcers to gather data about offers of infringing goods and services made through online advertising on these services.

The goal remains for consumers to be better informed, protected, and empowered. The text has ambiguities that the regulators will need to make work through interpretation and guidance, and legislators will need to resist the temptation to look “tough” by undermining the horizontal framework before it is even operational. It will take until at least the end of 2024—and probably more like 2025—to have a sense of whether these goals have been achieved. Hopefully, the legislation will provide a functioning framework for achieving safe and transparent online commerce, which then may inform how offline commerce is regulated as well. The framework of the DSA provides a first-of-its-kind regulatory toolbox which, if successful, will stand as an international benchmark for e-commerce regulation.

[73] Recitals 61 and 62, article 22.

Legend

	Obligation applies
	Obligation does not apply
MC	Mere conduit service providers
CP	Caching service providers
HP	Hosting service providers
OP	Online platforms
OTP	Online trading platforms
VLOP	Very large online platforms
VLOSE	Very large online search engine

		Intermediary Service Provider						
Art.	**New Obligations**	**MC**	**CP**	**HP**	**OP**	**OTP**	**VLOP**	**VLOSE**
9/10	Responding to orders from national authorities (either to act against illegal content or for information on service recipients) and informing affected service recipients.							
11/12	Publishing electronic point of contact details for Member State authorities, the European Commission and EBDS and, separately, for service recipients.							
13	If relevant, designating an EU legal representative, notifying the DSC and publishing contact details.							
14	Detailing content moderation policies in service T&Cs and considering the rights of all parties involved when enforcing them.							
15	Publishing annual transparency reports detailing content moderation activities.*							
16	Implementing electronic notice mechanisms (i.e. enabling anyone to flag suspected illegal content on the service) and taking decisions in respect of notices submitted.							
17	Providing a detailed statement of reasons to affected service recipients for certain decisions.**							
18	Reporting suspicions of life/safety-threatening criminal offences to law enforcement.							
20	Providing service recipients with access to an internal complaints-handling system and informing complainants without undue delay of decisions.***							
21	Publishing the right to have access to (and engaging in) out-of-court dispute settlement (i.e. for decisions on alleged illegal content, infringement of T&Cs and unresolved complaints).***							
22	Prioritizing and deciding notices from trusted flaggers without undue delay.***							
23	Enforcing suspension measures against abusive service recipients and notices/complaints.***							
24	Supplementing Art. 15 transparency reports with additional information and sending each decision and statement of reasons per Art. 17 to the European Commission without undue delay.***							
24	Publishing information on average monthly active EU service recipients and, on request, providing this (and calculations) to the DSC of establishment and European Commission.***							
25/26/28	Preventing targeted advertising using special category personal data (or any personal data of minors) and the use of dark patterns.***							
26	Providing service recipients with certain real-time ad transparency information and functionality to declare commercial communication content.***							
27	Providing transparency information in service T&Cs about recommender systems, and implementing functionality to select and modify preferred options.***							
30	Vetting and storing certain KYBC information before allowing traders to promote/offer products or services to EU consumers and making certain trader information available to service recipients.***						(if OTP)	
31	Enabling traders to provide certain compliance information, assessing the information, and undertaking random checks to verify if the products/services have been identified as illegal.***						(if OTP)	

32	Informing affected EU consumers of identified illegal products/services offered by traders through the service (or publishing this information if contact details are not held).***						(if OTP)	
34	Carrying out annual risk assessments, preserving related documentation, and, on request, providing the documentation to the European Commission or DSC of establishment.****							
35	Implementing mitigation measures to address the systemic risks identified in risk assessments (considering, in particular, the impact of those measures on fundamental rights).****							
36	Assessing and applying measures pursuant to crisis decisions from the European Commission.****							
37	Submitting to annual, independent audits (i.e. to assess DSA compliance), ensuring a written audit report is produced, and taking certain actions in respect of non-positive audit findings.****							
38	Providing at least one option in recommender systems not based on profiling.****							
39	Publishing a repository containing transparency information regarding each ad presented.****							
40	Providing access to data and explaining algorithmic/recommender systems to the DSC of establishment or European Commission on request (to assess DSA compliance), providing vetted researchers access to data (to research systemic risks in the EU and mitigation measures) and certain other researchers to publicly accessible data (to research systemic risks in the EU).****							
41	Establishing an independent compliance function to monitor DSA compliance, communicating the head of the function's details to the DSC of establishment and the European Commission, and ensuring compliance officers perform certain mandatory tasks.****							
42	Publishing enhanced transparency reports every six months and sending to the DSC of establishment and the European Commission (and publishing) certain other reports.****							
43	Paying the European Commission an annual supervisory fee for each designated service.****							

* Exemption applies for micro/small enterprises, unless they qualify as VLOPs.

** Exemption applies: (i) where the service provider does not have the contact details of the affected service recipient(s); (ii) in respect of deceptive high-volume commercial content (i.e. broadly content disseminated through intentional manipulation of the relevant service, in particular through the use of bots or fake accounts or other deceptive uses of the service); or (iii) if the restrictions are imposed due to an order to act against specific item(s) of illegal content from the relevant national authorities under Art. 9.

*** Exemption applies for micro/small enterprises, unless they qualify as VLOPs. The exemption continues to apply for 12 months after an OP or OTP no longer qualifies as a micro/small enterprise, unless they also qualify as a VLOP.

**** Under Art. 33, these obligations apply (or cease to apply) to VLOPs and VLOSEs from four months following notification from the European Commission of their designation as (or that they are no longer) a VLOP or VLOSE. The European Commission must terminate the VLOP/VLOSE designation if, during an uninterrupted period of one year, the OP or online search engine does not have a number of average monthly active recipients of the service equal to or higher than 45m (as may be adjusted).