# EU Digital Services Act: How to Approach Compliance

Teneo Insights / July 2022

**Paolo Cesarini**
Senior Advisor
Paolo.Cesarini@teneo.com

**The Digital Services Act (DSA) is getting closer to its final adoption. Strategic planning, proactive engagement in co-regulatory and standardisation processes and a track record of best efforts to comply, can help digital service providers prepare for EU-wide enforcement of new standards applicable to global companies.**

After more than a year of negotiations, the European Parliament and EU Member States reached a political agreement on the DSA in April and the European Parliament adopted the amended text with a large majority on 5 July. The Council's approval is expected by September 2022. Once adopted, the DSA will set new standards for all digital service providers. Its objective will be to foster responsible and diligent online behavior, ensuring a safe, predictable and trustworthy digital environment where fundamental rights will be safeguarded and innovation will thrive.

Together with its sister legislation, the Digital Markets Act, the DSA will profoundly impact the way digital players conduct their business. It will

impose sweeping new obligations for different types of providers while maintaining the basic tenets of the 2000 eCommerce Directive. It will also provide the basis for a novel co-regulatory approach, encouraging industry to adopt voluntary codes of conduct and standards in areas where cooperation between larger and smaller platforms will prove to be key in fully achieving the objectives of the law.

The strengthened Code of Practice on Disinformation, announced by the Commission on 16 June, is a good example of the type of eco-systemic approach that the DSA seeks to promote. Converging commitments by online platforms and other actors, including ad tech, media and civil society organisations, have proven necessary in order to complement the DSA's service-specific obligations and effectively tackle complex societal harms such as disinformation.

Companies will not have much time to adapt as, once approved, the DSA will be directly applicable throughout the EU after 15 months from its publication in the Official Journal, or from 1 January 2024, whichever is later. Very large online platforms (VLOPs) and search engines with more than 45 million users in the EU, or reaching more than 10% of the EU population, will have to comply even sooner, only four months after their designation.

Below are some practical steps that companies in scope of the DSA should consider now to be prepared in time.

## Set up service-specific compliance plans

The DSA will apply to a variety of digital services, including marketplaces, app stores, collaborative economy networks, content-sharing platforms and social media, regardless of their place of establishment. Companies with a "substantial connection" to the EU (i. e., with a registered seat, office, place of residence of company's legal representatives, or a significant number of users in the EU, or with activities targeted towards one or more Member States) will have to abide by a range of new, service-specific due diligence obligations, which will depend on the nature of their business, their size and their impact on the online ecosystem. VLOPs will be subject to stricter requirements in view of the systemic risks that their services may entail for citizens, businesses and society at large.

As a result, the new regulatory framework will force all online intermediaries, except micro or small enterprises, to review and adjust their operating methods by addressing at least the following three dimensions.

- **Risk-management and internal control processes.** At the core of the DSA is the objective of curbing the online distribution of illegal content, products and services, while protecting users' fundamental rights. To ensure that access to illegal content is swiftly disabled and take-down decisions are well-justified and fair, service providers will have to introduce easily accessible, user-friendly, electronic processes giving users the possibility to flag alleged breaches of the law. They will have to diligently deal with such notices, set up complaint and redress procedures, as well as out-of-court dispute settlement mechanisms, and cooperate with so-called trusted flaggers, i. e., public or private entities with expertise and competence in tackling illegal content. Specific additional requirements will apply to various types of intermediaries. For example, marketplaces will have to set up new processes to vet the credentials and ensure traceability of traders, while also taking effective measures against rogue actors. VLOPs will be expected to analyse any systemic risk stemming from the use of their services and to adopt effective mitigating measures, subject to mandatory data disclosures and independent audits. They will have to

introduce transparent policies preventing the viral spread of illegal content, develop best practices for content moderation limiting the online dissemination of harmful content, and, more generally, tackle the potential harm that their services may cause to civic discourse, electoral processes, public security and their users' physical and mental well-being.

- **Service design and business models.** The DSA will also involve significant changes to the design of certain platforms' products and features. Firstly, new transparency requirements for commercial and political ads (labelling, identification of sponsors, amounts spent, targeting criteria, creation of publicly accessible ad repositories) will apply to providers of online ads. Moreover, the DSA will outlaw the targeted advertising of minors based on profiling. It will also ban the use of certain categories of sensitive personal data for the purposes of behavioural advertising, such as sexual orientation or religious beliefs. Secondly, algorithms used in recommender and content ranking systems will have to be clearly explained in the platforms' terms and conditions, and VLOPs will have to re-engineer their systems to provide options for users that do not involve profiling. Thirdly, online interfaces and other functionalities managing user-service interactions will have to be reassessed and possibly modified in order to exclude dark patterns, such as build-in features that may impair the ability of users to make free and informed decisions.

- **Organisational structures.** The implementation of due diligence obligations will be subject to regular transparency reporting and duties of cooperation with national authorities. This will likely represent a relatively heavy administrative burden for all companies in scope, who should be ready to reassess the adequacy of their organisational structures and allocate sufficient resources to relevant tasks. For VLOPs, the DSA will require the creation of a new compliance function with authority, stature and direct access to top management.

Given the complexity of these new legal requirements, all companies in scope should consider setting up service-specific compliance plans with clear objectives, relevant measures and timeframes in advance, notably focusing on the areas outlined above.

## Engage in self-regulatory and standard setting efforts

The new legislation gives the European Commission the power to invite any online platform or search engine to participate in the application of complementary codes of conduct. Refusal to participate without proper explanation could be considered when determining possible breaches of the regulation, with obvious negative consequences for the companies concerned. The regulation explicitly refers to existing self-regulatory codes in areas such as consumer protection (the Product Safety Pledge and the Memorandum of Understanding against Counterfeit Goods), illegal hate speech and disinformation. But it also refers to the development of new codes of conduct that may prove necessary to address other areas of concern, such as illegal content (other than hate speech), online advertising, protection of minors, accessibility for users with disabilities and responses to crisis situations.

In the same vein, the Commission may also promote voluntary standards to support smaller providers of intermediary services in complying with the new rules. Such standards may cover certain technical procedures where the industry could define specific templates for the submission of notices, application programming interfaces, terms and conditions or audits. In the future, standards could also

cover commercially sensitive areas such as online advertising or the transparency and accountability of algorithms.

All companies in scope of the DSA should carefully consider the risks and opportunities that the development of codes of conduct and standardisation processes may represent for them. Timely participation in such initiatives would be key for any relevant player to minimise compliance costs and steer the processes towards desirable outcomes. A proactive approach would also help build a robust compliance track record and enhance reputation.

### Build a robust compliance track-record

Negotiations between the co-legislators have brought substantial changes to the enforcement system initially proposed by the Commission, amid fears that strict adherence to the country-of-origin principle could lead to under-enforcement, as seen with the implementation of the GDPR. The compromise solution consists of national and EU-level cooperation, whereby each Member State will give a Digital Services Coordinator responsibility for supervising the intermediary services established on its territory, while the Commission will have sole jurisdiction over VLOPs.

To ensure effective compliance, the competent authorities will enjoy extensive supervisory powers, similar to those under current anti-trust rules, including investigations and the ability to impose fines of up to 6% of worldwide turnover. While the imposition of large fines may concern only cases involving very serious breaches of the regulation, competent authorities will also have the power to seek effective and credible commitments from service providers to address specific objections. The latter will likely be the approach applied in a larger number of cases considered under the DSA.

These elements point to the need for companies to prepare in advance for possible enforcement actions, either at the national or EU level. As many of the DSA provisions break new ground, legal certainty will rest on specific solutions emerging from case law. In this context, investigations will involve a regulatory dialogue between the investigating body and the company. Companies should engage constructively in this process.

To do so, it will be important to rely on solid evidence, built up in advance and demonstrating good-faith adherence to the rules from the outset. This means that all policy changes enacted by a company to ensure compliance should be meticulously collected and documented. In particular, setting out baseline scenarios and progressive steps taken pursuant to dedicated compliance plans, combined with measurable service-level performance indicators where possible, could help build a credible track record and steer future investigations towards pragmatic solutions.

## Teneo is the global CEO advisory firm.

We partner with our clients globally to do great things for a better future.

Drawing upon our global team and expansive network of senior advisors, we provide advisory services across our five business segments on a stand-alone or fully integrated basis to help our clients solve complex business challenges. Our clients include a significant number of the Fortune 100 and FTSE 100, as well as other corporations, financial institutions and organizations.

Our full range of advisory services includes strategic communications, investor relations, financial transactions and restructuring, management consulting, physical and cyber risk, organizational design, board and executive search, geopolitics and government affairs, corporate governance, ESG and DE&I.

The firm has more than 1,500 employees located in 40 offices around the world.

**teneo.com**