KYRIAKIDES GEORGOPOULOS
LAW FIRM




INTERNET & E-COMMERCE

# Implementing the Digital Services Act- A Compliance Roadmap for Online Platforms and Marketplaces

June 16, 2026

# Implementing the Digital Services Act- A Compliance Roadmap for Online Platforms and Marketplaces

BY ANASTASIA DRITSA, IO LIGERAKI, PANAGIOTIS DAVAKIS

More than two years after its entry into force in November 2022, the Digital Services Act ("**DSA**") entered into force has been fully **applicable since February 2024** and has within such period of time fundamentally reshaped the regulatory landscape for digital services across the European Union.

The DSA forms part of the EU's broader strategy to harmonise digital regulation. It introduces a comprehensive, technology-neutral framework of obligations aimed at ensuring a safe, predictable and trusted online environment by addressing illegal content and societal risks while safeguarding fundamental rights. It also reduces market fragmentation, enhances legal certainty and supports innovation and the growth of digital services in the internal market.

Its scope is deliberately broad, capturing a wide range of intermediary services, including marketplaces, social media networks, app stores, and online travel and accommodation platforms. Under the DSA, obligations depend on the **type of service provided**, rather than on the provider itself. As a result, if a provider offers several different services, it may face different obligations under the DSA.

The Regulation adopts a **pyramid-like structure** consisting of different layers. The lower layer is the widest one and sets the rules applicable to the providers of all types of electronic services. The following layers introduce additional obligations to (i) providers of hosting services (second layer), (ii) online platforms/ marketplaces (third layer), and (iii) to Very Large Online Platforms and Search Engines (VLOP/VLSE) (top layer).

The obligations under the DSA are cumulative, meaning providers falling within a higher category must also comply with the obligations applicable to the lower layers of the pyramid. For example, an online platform must comply, not only with the obligations under the third layer, but also with those for providers of hosting services (second layer) and those offering more generic services (lower layer).

At national level, Greece has implemented the DSA through Law 5099/2024, designating the Hellenic Telecommunications and Post Commission (**EETT**) as the Greek Digital Services Coordinator and establishing enforcement mechanisms and sanctions for non-compliance.

Against this background, platforms and marketplaces can no longer view the DSA compliance as a future regulatory challenge. The focus has now shifted to implementation. This newsletter outlines the key steps that online platforms and marketplaces operating in Greece/EU should consider when assessing and building their compliance framework.

**Step 1 – Determine the DSA Classification**

The first compliance exercise is understanding where the service sits within the DSA framework.

As explained, the regulation follows a layered approach, meaning that obligations increase depending on the nature of the service provided.

For platforms and marketplaces, as a practical starting point, businesses should assess whether users can upload content, interact with other users, publish information visible to the public (online platform), or conclude contracts through the platform interface (online marketplace). The answer to these questions will usually determine the applicable responsibilities.

**Does the DSA Apply to Non-EU Platforms?**

One of the most significant features of the DSA is its broad territorial scope. The Regulation applies not only to providers established within the European Union, but also to businesses located outside the EU, having a substantial connection to the Union. Such a connection may arise where a provider has an establishment in an EU Member State, serves a significant number of users within the EU, or specifically targets EU markets through factors such as local languages, currencies, delivery options or country-specific domains. As a result, many non-EU platforms and marketplaces that offer services to users in Greece or elsewhere in the EU may find themselves subject to the DSA's requirements within Greece or the EU,despite having no physical presence within the Union.

**Step 2 – Build the Necessary Compliance Infrastructure**

Once the regulatory status of the platform has been identified, attention should turn to governance.

One of the most significant changes introduced by the DSA is the expectation that platforms maintain clear and effective channels of communication with both users and public authorities. Every provider must establish a single **point of contact** that allows users, regulators and competent authorities to communicate directly with the platform through electronic means.

At the same time, businesses should review their **terms and conditions**. Under the DSA, however, they have become a key compliance instrument. Platforms are expected to explain in a clear and transparent manner how they moderate content, restrict accounts, process complaints and apply their internal policies.

Platforms should identify who within the organization is responsible for DSA compliance. Providers with establishments in third countries who offer services in the EU must designate a **legal representative** in one of the Member States where they offer their services and inform the authorities accordingly.

**Step 3 – Implement Effective Notice-and-Action Procedures**

The DSA does not impose a general obligation on platforms to monitor or proactively supervise all content uploaded by users. Instead, providers are generally required to act when they obtain "**actual knowledge**" of illegal content. In practice, actual knowledge arises through user reports, orders from competent authorities or the platform's own investigations. Merely knowing that a service may contain illegal content, or using automated indexing, search or recommendation functionalities, is not sufficient to establish such knowledge. As expected from the DSA, providers must be able to determine whether the content is manifestly illegal without a detailed legal examination. Once a provider obtains actual knowledge of illegal content or activity and fails to act expeditiously, it may lose the benefit of the liability exemptions available under the DSA.

Consequently, platforms that publicly host user-generated content must provide **mechanisms** through which users and authorities can notify them of allegedly illegal content. These mechanisms must be easily accessible and designed in a way that allows sufficient information to be submitted for a meaningful assessment.

In practice, businesses should develop an **internal workflow** that ensures reports are received, reviewed and documented in a consistent manner. Once a notice is submitted and deemed valid, the platform is expected to assess the content diligently and take appropriate action without undue delay.

Equally important is the obligation of the provider to communicate relevant decisions to the users of the service. Where content is removed, access is restricted or an account is suspended, users should receive a **statement explaining the reasons** for the decision and the available means for redress (SoR).

Users who are affected by content moderation decisions must have access to mechanisms allowing them to **challenge** those decisions. Platforms and marketplaces are therefore expected to establish internal **complaint-handling** systems through which users can contest actions such as content removals, visibility restrictions or account suspensions. From an operational perspective, businesses should ensure that complaints can be submitted easily, reviewed by appropriately qualified personnel and resolved within a reasonable timeframe. **Automated systems** may assist the process, but meaningful human oversight remains essential.

The quality of the process often matters as much as the outcome itself. Regulators increasingly expect platforms to maintain **clear records** demonstrating how notices were handled, who reviewed them and why particular decisions were reached.

**Step 4 – Marketplace Operators Face Additional Responsibilities**

Businesses operating platforms in the form of online marketplaces should pay particular attention to an extra layer of obligations introduced by the DSA concerning trader traceability and trading of illegal products.

One of the regulation's central objectives is to improve the **traceability of traders** operating through digital marketplaces. As a result, marketplace operators are required to collect and verify specific information before allowing traders to offer products or services through their platforms. Marketplace operators should therefore review their onboarding procedures and ensure they are capable of verifying the identity and legitimacy of traders.

The DSA also requires marketplaces to take action when they become aware that **illegal products or services** have been offered through their platform and notify users on a) the fact that a product/ service is illegal, b) the identity of the trader, c) any relevant means of redress.

The European Commission's recent enforcement action against **Temu** demonstrates the increasing scrutiny faced by online marketplaces under the DSA. The Commission, primarily responsible for the monitoring and enforcement of the additional obligations applying to the biggest platforms and search engines, imposed a **€200 million fine** after concluding that Temu had failed to properly identify, assess and mitigate the systemic risks associated with illegal products being offered through its platform.

According to the Commission, Temu's risk assessment relied largely on general information about the e-commerce sector rather than evidence specific to its own service and significantly underestimated the likelihood of EU consumers encountering illegal products. The investigation also highlighted concerns regarding the platform's recommender systems and promotional programs, which may have contributed to the dissemination of non-compliant products. The case serves as a reminder that **risk assessments** must be evidence-based, platform-specific and supported by effective mitigation measures.

**Step 5 –Transparency Obligations**

Beyond complaint handling, the DSA introduces extensive transparency obligations. Platforms and marketplaces are expected to **publish reports** describing how they moderate content, process notices, handle complaints and apply automated tools. Although these obligations are often viewed as administrative exercises, they can become challenging if the necessary data has not been collected throughout the year. On that note, a further aspect that is often overlooked is the **DSA Transparency Database**. Online platforms are generally required to register and submit statements of reasons whenever they remove content, restrict visibility or otherwise take moderation measures against users. As enforcement activity increases, businesses should ensure that their internal processes can retain the information required for these reports/submissions.

**Step 6 – Greek Dimension**

Businesses targeting users in Greece should also assess their obligations under the **national framework** implementing and enforcing the DSA together with the respective EU procedure. In particular, providers should assess according to specific criteria (i.e. provider size and annual turnover) whether registration with the **EETT Registry of Intermediary Service Providers** is required and ensure that any communications with national authorities can be handled efficiently.

This national layer should not be overlooked during implementation projects. It is increasingly becoming a focus area during compliance reviews and regulatory assessments by the competent authority.

**Final Thoughts**

The DSA is best not viewed as a standalone legal obligation or a one-off compliance exercise. Instead, it represents a broader shift towards **greater accountability in the digital economy**. The European Commission has made clear that it expects platforms and marketplaces to move beyond formal compliance and actively manage the risks arising from their services.

For platforms and marketplaces operating in Greece and the EU in general, successful implementation requires more than updating legal documentation. It requires the creation of governance structures, operational procedures and internal controls capable of demonstrating compliance on an ongoing basis.

As DSA enforcement continues to intensify across the EU, businesses that take a proactive approach today will not only reduce regulatory risk but will also strengthen user trust, improve operational resilience and position themselves more effectively in an increasingly regulated digital environment.

# Contact Us



Anastasia Dritsa
**PARTNER**

*A.dritsa@kglawfirm.gr*

*Follow Us*

**ATHENS OFFICE**

28, Dimitriou Soutsou Str.,
115 21 Athens

T +30 210 817 1500
E kg.law@kglawfirm.gr

**THESSALONIKI OFFICE**

31, Politechniou Str.,
551 34 Thessaloniki

T +30 2310 441 552
E kg.law@kglawfirm.gr

*www.kglawfirm.gr*

**Disclaimer**: This newsletter contains general information only and is not intended to provide specific legal, or other professional advice or services, nor is it suitable for such professional advice, and should not be used as a basis for any decision or action that may affect you or your business. Before making any decision or taking any action that may affect you or your business, you should consult a qualified professional advisor. We remain at your disposal should you require any further information or clarification in this regard.

**©Kyriakides Georgopoulos, 2026**