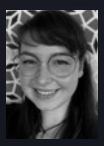
From regulation to reality: the DSA's early impact on trust and online safety

Manon van Rietschoten
is a director at KPMG IT Assurance & Advisory.



Angelica van Beemdelust
is a consultant in the KPMG NL Responsible AI team.

Koen Klein Tank
is a partner at KPMG IT Assurance & Advisory.

Designated very large online platforms (including social media, marketplaces, classifieds) and online search engines were required to publish their first audit reports by 28 November 2024. The results show that a wealth of work has been done over the last few years to comply with the Digital Services Act (DSA), but online platforms cannot rest as we see "negative" assurance reports (with adverse and qualified opinions) for 18 out of the 19 online platforms subject to the DSA requirements in the first audit year. This article discusses what the DSA has achieved since its introduction and how it will further shape online trust, safety, and protection of users of these online platforms.

INTRODUCTION

The European Commission (EC) has enacted several digital regulations over the last couple of years, one of the most influential is the Digital Services Act (DSA). The DSA is one of the frontrunners in global legislation with the aim to provide a safer and fairer digital environment for online users and is part of a broader legislation package (more than 120 laws and regulations) introduced by the EC related to the digital single market. This regulation introduces clear rules for online platforms, aiming to protect users from illegal content, misinformation, and harmful practices, while also ensuring fundamental rights are respected across all EU member states.

The DSA imposes rules and regulations with cumulative obligations for (major) online intermediaries. The smallest scope of obligations applies to all intermediaries with gradually more requirements for hosting services, online platforms, and finally, very large online platforms (VLOPs) and very large online search engines (VLOSEs) with the largest scope, the latter being differentiated by the number of monthly users in the EU with a threshold of 45 million. The EC initially designated 19 VLOPs and VLOSEs in May 2023, among them Amazon, Zalando, Facebook, TikTok, Bing, and Google Search. Over the last year, an additional 6 have hit the VLOP and VLOSE threshold bringing the total to 25 as of 31 October 2024.

At this largest scope of requirements, we see the need to perform annual, thorough risk assessments to identify and address systemic risks associated with illegal content, fundamental rights, electoral processes, and user protection. VLOPs and VLOSEs must also

1. publish transparency reports detailing their content moderation activities and implementation of measures to safeguard minors and vulnerable people;
2. consider the design of their algorithms and recommendation systems when evaluating these risks, and
3. contract an independent auditor to perform a yearly audit and publish the audit reports on their websites.

We can now see the results of the first round of audit reports that online platforms had to publish by 28 November 2024.

WHERE ARE WE TODAY?

While no fines have been imposed yet, the results of the audit reports show that there is still significant work to be done by the online platforms as the audit firms concluded for several obligations that the measures in place are not sufficient yet.

Particularly, we see online platforms struggling with implementing all necessary controls to meet the stringent standards set by the DSA. Online platforms had limited time to prepare for the DSA audit as the final version of the Delegated Act on performing audits was released in the year one audit period. Moreover, often platforms had limited experience in implementing extensive control frameworks for the areas in scope of the audit, let alone being audited. Most notably, the audit reports reveal that the online platforms have challenges to show to their auditor how they have implemented measures around transparency reporting. Other areas of contention include the recommender systems, notice and action mechanisms for content moderation, and online protection of minors.

HOW IS THE DSA EFFECTIVE?

With the audit reports primarily accentuating the areas that can be improved, we also want to highlight areas where the DSA has already shown its effectiveness. Perhaps as a user of online platforms, you have received emails in your inbox about upcoming changes in the terms and conditions, or you may have noticed that the top pages as a result of your search query are marked as sponsored advertisements. These are both demonstrations of increased public transparency, a direct result of the DSA's transparency requirements. Online platforms have also been publishing transparency reports, directly accessible on their website, in which they report on illegal content, content moderation activities, and number of users on their platform.

One of the biggest changes that the DSA has brought forth so far, amongst other regulations in the online trust and safety space, is the notable shift toward more compliance initiatives. For example, we see an increased priority for compliance within the board of management and the more operational teams including the engineers. The DSA mandates the establishment of a dedicated compliance function, which has led to the hiring of compliance officers to ensure adherence to this law. Consequently, second line of defense teams are growing within these online platform providers. There is now more emphasis on risk management with measures for risk mitigation being prioritized and compliance becoming more embedded in their processes, for example, in the design and development processes.

Conversely, a major challenge is to minimize any delays that may occur in launching new or updated features and products. It becomes a careful balancing act of continuing to drive innovation while ensuring that risks are carefully considered. This shift towards cautious and deliberate implementation indicates a maturing digital

landscape that prioritizes online safety and trust. We have observed that the introduction of new online products or new product features that are subject to EU Acts, such as the DSA, DMA or upcoming AI Act, has been slowed down or postponed recently.

A POSITIVE BEGINNING WITH ROOM FOR IMPROVEMENT

While risk management and compliance moved up the priority ladder, the DSA is a sudden and challenging law to comply with so quickly after its adoption. Few prior regulations at the national level existed for online safety unlike what can be seen in the financial industry. Moreover, the DSA can be interpreted in various ways, for example, online platforms can define for themselves how they interpret terms like "easy to access" and "user friendly". So, not only is the DSA new and difficult to adhere to on such short notice, it also isn't clear-cut in particular areas.

Additional guidance, the closing of EC investigations, new Delegated Acts, and future case law will all help bring desired clarity to the more ambiguous areas. Also, the EC is expected to encourage online platforms to voluntarily become a signatory for upcoming Codes of Conduct such as requiring age verification to protect minors, promoting safe online advertising, countering illegal hate speech, and combatting the spread of disinformation. The Codes of Conduct are a practical tool the EC can leverage to pressure online platforms to implement measures against the systemic risks imposed by their services.

Another area we hope to see results in over the coming years is the requirement to provide researchers with access to data on the platform. This could, for example, help researchers contextualize DSA requirements by highlighting the social impact of the risk management decisions of online platforms.

All of these steps should lead to a more comprehensive framework for online safety and trust within the EU.

THE DSA IS NOT THE ONLY LEGISLATION IN THIS FIELD

The DSA is not the only legislation on online safety within the EU or globally. Most recently, we see the United Kingdom and Australia both publishing online safety acts as well as Ireland with the Online Safety Code. We've also seen an uptick globally in recent years of laws and regulations contributing to online safety in the privacy, competition, and artificial intelligence (AI) spaces.

On the privacy and data protection side, the EU General Data Protection Regulation has been in force since 2018, and the United States (U.S.) continues to see state-by-state privacy laws enacted (as the first US federal Privacy Bill is still in the legislative process). For online platforms that act as gatekeepers, the Digital Market Act (2022) is key in regulating digital platforms to ensure fair competition. Furthermore, the EU's AI Act (2024) will be an important contributor to a more robust online safety legislative framework and, again, we see the U.S. introducing AI regulations of its own. Adding to this challenge, we see contradictory trends globally where certain requirements that are mandatory in one jurisdiction (e.g. EU), e.g. content moderation, could be(come) relaxed or forbidden in others (e.g. US).

WHAT WILL THE FUTURE BRING?

Drawing from our experience with the majority of the designated online platforms, we anticipate that over time, the maturity of compliance processes will increase and transition to a more routine mode of operation.

As the EC develops more guidance, implements more Delegated Acts, EC investigations are concluded, Codes of Conduct are developed and converted under the DSA, case law is formed, and research on online safety is published, the specific requirements of the DSA will become clearer and the regulatory framework more defined. As a result, this will heighten compliance scrutiny for online platforms and provides less flexibility in the interpretation of requirements in the law.

The DSA is a sudden and challenging law to comply with so quickly after its adoption

CONCLUSION

The DSA is a solid steppingstone towards a safer and more transparent digital online environment for users. However, it will take several years for the dust to settle and before we know what the DSA – and other online trust and safety regulation within and outside the EU – has achieved. So, while online users may experience a first wave of online safety and protection benefits, it remains to be seen whether the DSA will ultimately provide a significant overall benefit for internet users and society at large.

About the authors

Manon van Rietschoten is a director at KPMG IT Assurance & Advisory. With extensive experience in IT assurance and related advisory engagements, she is working within the financial sector and for online platforms. Her skills encompass IT Audit (RE and RA qualifications), Technology Assurance (ISAE 3000, ISAE 3402) and related advisory engagements. She is passionate about enhancing the safety of our online world.

Angelica van Beemdelust is a consultant in the KPMG NL Responsible AI team. She is specialized in AI governance, policy and risk management, with extensive experience and expertise in IT and AI Assurance.

Koen Klein Tank is a partner at KPMG IT Assurance & Advisory and serves as the Global KPMG lead for Digital Services Act (DSA) and Digital Markets Act (DMA) assurance services. Additionally, he chairs the Technology Working Group of the European Contact Group (ECG). The ECG represents the six largest international professional services networks in Europe: BDO, Deloitte, EY, Grant Thornton, KPMG, and PwC. The working group prepares FAQs, illustrative drafts of audit reports, and develops audit guidance for regulations such as the DSA and DMA.