SQUIRE PATTON BOGGS

Algorithm Audits

EMEA – 4 December 2023

Introduction

On October 20, 2023, the European Commission adopted the delegated act on independent audits under the EU's landmark Digital Services Act (DSA). The delegated act aims to lay down the "rules of engagement" for auditors and platforms subject to these audits, which are one of the essential requirements under the DSA for affected online platforms and search engines. This novel framework presents both opportunities and risks for companies as they navigate these new audit obligations and the broader DSA landscape.

DSA Requirements

The DSA requires that very large online platforms (VLOPs) conduct annual systemic risk assessments of online harms and take appropriate mitigating measures. The DSA also requires VLOPs that use recommendation systems to reveal in their terms of service the primary parameters used by algorithmic amplification systems. In addition, the DSA requires VLOPs to submit yearly external audits to certify that they have complied with these risk mitigation and reporting requirements, and mandates that the auditors conduct an independent risk assessment. Moreover, "very large online search engines" (VLOSEs) are subject to increased due diligence obligations as part of the mandatory, yet self-regulatory regime of the DSA.

What Is an Algorithm Audit?

Recital 5 of the delegated act lays out that annual independent audits should be aligned with yearly risk assessments, making the outcomes of the independent audits and risk assessments inextricably linked. Together, they mark one of the first formal compliance activities under the DSA, and it is important to understand them in context. The risk assessments, mitigation strategies and independent audits required by the DSA are linked to the other activities, policies and procedures that VLOPs and VLOSEs must adopt under the DSA. The audits will ultimately evaluate VLOPs' and VLOSEs' compliance with this broad sweep of provisions, and, crucially, it remains unclear what standards auditors will be expected to apply to the auditing of the risk assessments (or any other part of the DSA) as they conduct their evaluations.

What Is ECAT?

Central to the risk assessment, auditing of algorithmic systems and ultimately determining compliance, will be the newly created European Centre for Algorithmic Transparency (ECAT), which is tasked with providing technical expertise for the European Commission in its supervisory and enforcement role. This task could be made more difficult given that the ECAT will likely have to evaluate a wide variety of audits conducted on a range of VLOPs and VLOSEs. With so little clarity on what standards auditors or the commission should apply, or on precisely how ECAT will be concretely contributing to this process, companies have an opportunity to use the first submissions and related engagement with regulators to better inform ECAT's own internal processes and shape what algorithmic auditing and transparency in the DSA means in practice.

Broader Context

Other EU laws or initiatives that are part of the algorithmic audit and transparency ecosystem include the Platform-to-Business Regulation and the New Deal for Consumers, which mandate disclosure of the general parameters for algorithmic ranking systems to business users and consumers, respectively. The General Data Protection Regulation (GDPR) sets rules for the profiling of individuals and related automated decision-making and gives users the "right to explanation" about algorithmic processes.

The EU Digital Markets Act obliges designated gatekeepers also to submit their techniques of data-profiling consumers to an independent audit. Moreover, the European Commission has expressed an interest in the use of algorithms under the lenses of antitrust legislation, in particular with regard to pricing and self-preferential algorithms, and has advocated in favor of compliance by design, including through the use of audits.

Finally, the EU draft Artificial Intelligence Act proposes a risk-based approach to AI regulation along a sliding scale of potential harms and requires that providers of high-risk AI systems conduct "conformity assessments" before their products enter the European market. This is an internal audit to ensure that governance of the AI is compliant with regulation. The act would also create a post-market monitoring requirement for high-risk AI systems. Very high-risk AI systems, defined as those intended for use in real-time or remote biometric identification, may require external audits. This approach to high-risk AI systems involves a combination of self-regulation, voluntary adherence to standards, and government oversight.

How We Can Help

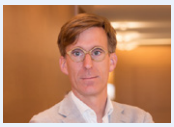
We have put together a team of specialists among our tech-sector lawyers and public policy advisers with the demonstrated expertise to navigate these issues effectively and efficiently. This team has extensive experience – including as regulators at the European Commission, in-house in Big Tech companies and in private practice – with risk assessments and audits covering multiple broad categories of risks, including the spread of illegal content, negative effects on fundamental rights, negative consequences for civic discourse, public security, and individuals' physical and mental wellbeing, as well as other adverse outcomes for consumers and competition. In particular, our team is able to draw from its experience with antitrust risk-based audits that are very similar in nature to the type of risk-based audits expected under the DSA – and very different from a simple box ticking exercise.

The independent auditing of VLOPs and VLOSEs' algorithmic systems comes with its own opportunities and risks. In the absence of a clear definition of "systemic risk" in the text of the DSA, or guidelines on how to conduct risk assessments, our team has developed a framework to capture a broad definition of risks that impact multiple, interdependent fundamental rights, including multiple different appropriate and coordinated assessment tools, resulting in a workable mixed-method approach to compliance. Our comprehensive and strategic approach – from initial shaping of a risk assessment protocol through ultimate agency submissions and engagement – leverages our deep understanding of regulators' concerns and the broader regulatory landscape, to develop practical solutions.

For the technical aspects of these independent audits, we are happy to partner with IT forensic analysts and other technical experts as appropriate. In addition, our work product would benefit from EU legal privilege protection.

If you would like to have a conversation with our team in confidence, please reach out to your usual contact at the firm or any of the DSA Audit team members below.

Contacts



Charles Helleputte
Partner
E charles.helleputte@squirepb.com

Francesco Liberatore
Partner
E francesco.liberatore@squirepb.com

Gorka Navea
Partner
E gorka.navea@squirepb.com

Martin Mackowski
Partner
E martin.mackowski@squirepb.com

Matthew Kirk
International Affairs Advisor
E matthew.kirk@squirepb.com