FEEDBACK ON THE DIGITAL SERVICES ACT'S DRAFT DELEGATED REGULATION

Rules on the Performance of Audits

June 2023

Introduction

The Computer & Communications Industry Association (CCIA Europe) is pleased to provide feedback to the European Commission on the draft delegated regulation (DDR)[1] laying down rules on the performance of audits for very large online platforms (VLOPs) and very large online search engines (VLOSEs), pursuant to Article 37 of the Digital Services Act (DSA).[2] In particular, Article 37(7) of the DSA states that the DDR should set out the rules on the procedural steps, auditing methodologies, and reporting templates for the audits that are to be performed.

Below you will find our recommendations on key elements of the DDR:

1. Preliminary remarks on first audits
2. Alignment with auditing standards
3. Potential deviations from the Digital Services Act
4. Further clarifications on the practicalities of the auditing process

I. Preliminary remarks on first audits

1. Approach to the first audit

The DSA is a novel regulatory regime which requires considerable investment by service providers into new systems, processes, and people. In recognition of this, and in line with the principle of proportionality, the DDR should explicitly recognise that the methodology deployed for the audit in the first year of DSA application will be different from that deployed in subsequent audits.

The DSA obligations (including the requirement to complete the risk assessment) only apply as a matter of law to VLOPs and VLOSEs from 28 August 2023. The first-year audit should accordingly focus on the appropriateness of the steps put in place to identify systemic risks and to build out the systems, processes, and teams required to address them. A clear distinction should be made between the existence of controls, which should be the focus of the first-year audit, and the effectiveness of those controls, which should be the focus of subsequent audits. The DDR does not, as presently drafted, take into account the potential need for the audit methodology to evolve from the first year to subsequent years, nor does it build in the flexibility to allow the auditing organisation to take that into account.

[1] European Commission, Have your say, Digital Services Act – conducting independent audits, available at: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13626-Digital-Services-Act-conducting-independent-audits_en

[2] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R2065&qid=1666857517641

While the DDR avoids an overly prescriptive approach, the instructions to conduct the audit should be fully aligned with Article 37 of the DSA. In the meantime, the DDR should clearly state that the auditing process has to rely on existing auditing practices and remain flexible enough to adapt to specific providers and obligations. Once the auditing process has matured, further clarifications might be required.

2. Time period for the first audit report

Given the complexity of simultaneously developing processes to audit compliance with a novel regulation, novel control frameworks, and standards for such audits, the audit for the first year should be conducted in a point-in-time manner. This will streamline the audit for both the service provider that is being audited and the auditing organisation, while also allowing the audit to proceed in an efficient manner given the limited period of time allocated to the first audit, and still ensuring that the audit thoroughly examines compliance with the DSA.

II. Alignment with auditing standards

1. Clear and flexible instructions for auditors

The DDR does not supplement Article 37 of the DSA enough in order to fully clarify the scope of the independent audits. Article 37(1) mentions that all obligations of Chapter III, commitments to codes of conduct (Articles 45 and 46) and crisis protocols (article 48) shall be assessed for compliance by auditors. Yet, some of the obligations still have ambiguous meanings.

The DDR does not provide an answer to how this assessment should be done in practice and leaves many elements to be determined according to the "professional judgement" of auditors. While section IV of the DDR gives examples of auditing methodologies and specificities for a few articles of the DSA, the scope of the audits remains broad and vague. Auditing organisations could face excessive difficulties in conducting compliance assessments of these obligations as long as their meaning is not settled. Leaving each auditor to determine which audit methodology to use could lead to disparate audit reports.

The DDR cannot ask auditing organisations to define the criteria for how to achieve compliance with the above-mentioned DSA obligations. Auditors are bound by professional standards – e.g. International Professional Practices Framework (IPPF) – which state that auditing organisations cannot give legal advice, but only assess compliance with the law. As long as some DSA requirements are not defined in sufficient detail to allow for proper auditing, they should be left out of the first-year audit reports. While the DDR should not adopt a prescriptive approach for each of the obligations that require to be audited, further clarity definitely is needed so that the audit reports can be reliable tools to assess DSA compliance.

Additionally, the DDR should clearly state that auditing organisations cannot be asked to give legal advice or engage in legal interpretation. Besides the fact that this already is an existing professional requirement, it would also ensure that audit reports do not differ due to inconsistent legal interpretations. The DDR should also state that auditors cannot suggest specific actions to providers to achieve compliance. Whereas auditing organisations can make "operational recommendations" to providers in the event of a non-positive audit

report, the DDR should make clear that the providers retain discretion over the exact actions they take to address those operational recommendations, in line with Article 37(6) of the DSA.

To solve this issue the DDR might benefit from a more progressive approach. For example, it could limit audit reports to binary obligations during the first years. Non-binary obligations could be progressively integrated into the audit reports, as regulators and courts provide more guidance on their legal interpretation. Audited providers would then be able to provide evidence of their compliance with these obligations so that the European Commission can decide on how they should be evaluated in the framework of audits, in line with Recital 12 of the DDR. The DDR should also clearly state which audit methodologies are acceptable (and, to the extent possible, not let those differ for each audited obligation or commitment in scope), rather than leaving this up to the auditing organisation's discretion.

2. Reasonable level of assurance

The DDR states that auditing organisations should express their audit opinions with a "reasonable level of assurance" and that conclusions should either be "positive", "positive with comments" or "negative" (Articles 3 and 8). It would be useful for the DDR to acknowledge that these terms should be understood in the context of relevant international auditing standards.

An "audit conclusion" for an individual DSA obligation, under Article 8(1) of the DDR, could still be recorded as "negative" just because – for a short time within the audit period – there was a compliance shortcoming, even though it was diligently remedied within that same timeframe. This would be disproportionate in many cases. A proportionality analysis should be applied in those cases and, at most, that instance should be characterised as "positive with comments" if the VLOP or VLOSE concerned was compliant for the larger part of the audit period.

Similarly, having a "positive with comments" or "negative" characterisation for compliance with a single DSA obligation would render the entire audit outcome as positive with comments or negative. Again, a proportionality analysis should be applied, taking a look at the VLOP's or VLOSE's compliance more holistically. The obligation-by-obligation breakdown of the audit report would still allow parties to have a closer look at particular obligations and compliance with those.

Absent these important amendments, the DDR would effectively set the industry up for failure and lead to significant reputational risks for VLOPs and VLOSEs that are unwarranted and disproportionate.

Furthermore, a reasonable level of assurance might not be appropriate given the nature of the compliance. This is particularly justified by the consequences providers face if a negative report is issued, as it will feed the regulator's decision on the overall compliance of the provider with the DSA as well as potential fines.

The DDR should also consider that imposing a reasonable level of assurance when (as previously stated) the audited obligations remain vague or subjective, might be a deterrent for auditing organisations. Alternatively, auditors might choose to take a conservative

approach to compliance, which would make receiving a positive conclusion close to impossible. For example, the DDR asks for the societal and economic context to be taken into account in the audit risk analysis (Article 9). But this broad criterion leaves too much room for interpretation and potential influence on a process that should remain objective.

III. Potential deviations from the Digital Services Act

1. Selection of auditing organisation

Article 4 of the DDR puts the burden to check if auditing organisations fulfil the requirements of expertise and objectivity laid down in Article 37(3) of the DSA fully and squarely on audited providers, and them alone. However, putting this obligation on audited providers alone would be ineffective and disproportionate. While audited providers can contribute to the assessment regarding independence or conflicts of interest, they cannot solely decide if auditing organisations fulfil all requirements. Besides, the DSA does not state that audited providers should be responsible for checking if auditors respect these requirements. The consequences of the invalidation of an auditing organisation are not laid out in the DDR, creating legal uncertainty for providers.

Instead, the DDR should state that audited providers should rely on the adherence of auditing organisations to standards, certifications, accreditations, and self-declarations to prove that they respect the requirements of Article 37(3) of the DSA. Further guidance on whether an auditor or one of its subcontractors can intervene in several independent audits would also be welcomed.

2. Auditors' comments for improvements

In case an auditing organisation decides to issue "positive with comments" audit conclusions, Article 8(1)(b)(i) of the DDR indicates that auditors can recommend "improvements that do not have a substantive effect on its conclusion". This could lead auditors to issue recommendations that go beyond the scope of the DSA, as they do not relate to strict compliance with the DSA. Worse, as auditors take into account past audit reports, these types of recommended improvements could have a cumulative effect, increasing potential deviations from the DSA. To prevent this from happening, this particular reference should be deleted from the DDR. Alternatively, the DDR could clarify that any such recommended improvements do not amount to "operational recommendations" under Article 37(6) of the DSA.

3. Testing risk assessment assumptions with stakeholders

Article 13(1)(a)(v) of the DDR includes testing "whether and how assumptions on risks with groups most impacted by the specific risks" as one of the means to assess compliance with Article 34 of the DSA on risk assessments. However, Article 34 of the DSA does not list this type of requirement, while Recital 90 of the DSA merely points out that providers can consult independent experts and civil society organisations on their mitigation measures. This particular means of testing should therefore be removed from the list of Article 13 of the DDR.

4. Requiring assessments of applicability of Article 35 points (a)-(k) of the DSA

Article 14(1)(b) of the DDR pertains, among other things, to analysing "how the audited provider assessed whether the risk mitigation measures in Article 35(1) points (a) to (k) were applicable to the audited service and whether the conclusion of that assessment was appropriate, including as regards those measures which were not applied by the audited provider." However, Article 35 of the DSA does not require each measure in Article 35(1) points (a) to (k) to be assessed for applicability. Rather, it only states that "[p]roviders of very large online platforms and of very large online search engines shall put in place reasonable, proportionate and effective mitigation measures" and that "[s]uch measures may include, where applicable…". This provision should therefore be removed from Article 14 of the DDR.

IV. Further clarifications on the practicalities of the auditing process

1. Clarify terms necessary for the conduct of audits

Several terms used in the DDR should be further clarified. Article 14(1)(c) of the DDR states that audit reports should evaluate if mitigation measures (Article 35 of the DSA) are "reasonable, proportionate and effective for mitigating risks". However, the DDR lacks guidance on how to precisely assess how a mitigation measure can meet these criteria. That is why the DDR should provide guidance in this respect, so that providers and auditors can rely on a common understanding of these standards. This is important in order to ensure that providers are audited in a consistent and proportional manner. Given the complexity of this space, we suggest that the DDR calls for the further development of a standard for such audits and that the requirement that auditors specifically assess this requirement be delayed until such time as the standard exists.

Article 14(3)(b) of the DDR suggests that auditors can ask audited providers for information that exceeds the scope of Article 35 of the DSA. Instead, the DDR should limit this provision so that risk mitigation can only be understood as the meaning under the DSA. Article 14(3) should also be amended to make clear that auditors may access this information, but are not required to do so. Auditors should be able to access the information needed to provide reasonable assurance, but requirements that large volumes of documents be considered – whether deemed helpful to the audit or not – increase the cost and timeframes with no particular benefit to anyone. Article 14 of the DDR should also specify that auditors can only enquire about information relevant to the evaluation of compliance with the mitigation of risks.

2. Concerns regarding data sharing

Recital 13 and Article 5 of the DDR describe the cooperation and assistance between the audited provider and the auditing organisation. Audited providers are expected to give access to data, personnel, and premises to auditors, as well as those of "relevant sub-contractors". The provider will most likely be unable to grant access without the approval of the sub-contractors. This reference should either be removed or adapted as audited providers are simply not able to decide on their own whether to give access to data, personnel, or premises.

Furthermore, the type of data accessible to auditors is very broad, as it encompasses "any other necessary information", e.g. "personal data", "IT systems" or "internal decision-making process". This list of data should be further defined and limited to ensure it respects the rights of users and businesses. Internal information of the provider that is made accessible should only be relevant to DSA independent audits. Access to personal data should be granted under exceptional circumstances and with strict safeguards, only if auditors cannot evaluate compliance in any other way.

Auditing organisations are encouraged to conduct "analytical procedures [...] based on observations of processes and activities of the audited provider in designing, developing, operating, testing, and monitoring algorithmic systems" (Recital 29). This also raises concerns regarding the protection of confidential information, trade secrets, intellectual property rights, and the overall security of the services. Safeguards should be introduced to ensure that these rights are sufficiently protected. Further clarification would also be welcomed on Recital 30 in order to understand what the possibility to "gather information that the audited provider has not previously documented" exactly entails.

Finally, the DDR should acknowledge that data/information safeguards are necessary, particularly with respect to highly-sensitive information that pertains to the effectiveness of certain controls designed to address the harms set out in the DSA. If such information is provided to the Commission or an auditing organisation, and were to be subject to a leak, it could undermine the effectiveness of the control on a catastrophic scale. The DDR should thus acknowledge that it is possible for auditors to test and reach reasoned conclusions on the effectiveness of controls without seeing such information.

3. Format and frequency of reports

Two other uncertainties need to be clarified. First, Recital 5 of the DDR mentions the need to conduct audits more often than the annual ones required in the DSA. Further information, or examples of when these additional audits are necessary, would be useful for providers. Second, the Annexes providing the templates of the reports have many open-ended sections which could damage the comparability of reports between providers or over time. A streamlined labelling of each section could be useful to avoid inconsistencies.

4. Report on how compliance officers "made use of" controls

Article 14(2)(a)(iii) of the DDR requires the auditing organisation to "evaluate how the compliance officer or officers made use of those internal controls as part of their tasks." This obligation is unclear and unnecessary, and appears not to be restricted to auditing compliance with the DSA itself. Likewise, Article 13(2)(a)(iii) of the DDR requires the auditing organisation to "evaluate how the compliance officer or officers conducted those internal controls". It is not clear what would be evaluated here, but again, it appears unnecessary in light of Article 13(2)(a)(i)-(ii) of the DDR, which targets the controls more substantively.

Conclusion

CCIA Europe appreciates the European Commission's efforts to provide rules on the performance of audits by VLOPs and VLOSEs as early as possible in the compliance process. Our recommendations focus on improving the audit process with a view to making sure these audits are feasible for both service providers and auditing organisations. We remain available to further discuss our feedback with the European Commission.

About CCIA Europe

The Computer & Communications Industry Association (CCIA) is an international, not-for-profit association representing a broad cross section of computer, communications, and Internet industry firms.

As an advocate for a thriving European digital economy, CCIA Europe has been actively contributing to EU policy making since 2009. CCIA's Brussels-based team seeks to improve understanding of our industry and share the tech sector's collective expertise, with a view to fostering balanced and well-informed policy making in Europe.

For more information, visit: twitter.com/CCIAeurope or www.ccianet.org

For more information, please contact:
CCIA Europe's Head of Communications, Kasper Peters: kpeters@ccianet.org