Digital Services Act (DSA) Implementation

Feedback on the draft delegated act on data access for researchers

December 2024

Introduction

The Computer & Communications Industry Association (CCIA Europe) is pleased to present its feedback on the draft delegated act laying down the technical conditions and procedures under which providers of very large online platforms (VLOPs) and very large online search engines (VLOSEs) are to share data pursuant to Article 40 (hereinafter draft delegated act on data access) of the Digital Services Act (DSA).[1]

CCIA Europe appreciates the efforts of the European Commission to gather stakeholder input throughout the drafting process of this important piece of secondary legislation. First with a call for evidence in 2023, and now with the ongoing consultation on the draft delegated act. The data-access requirements of Article 40 of the DSA are an unprecedented transparency exercise in EU law. Achieving a balance between enabling researchers to access data and protecting the fundamental rights of users and companies is the biggest challenge in making sure this provision is successfully implemented.[2]

CCIA Europe recommends several improvements to the draft delegated act to make sure that this balance is upheld throughout the whole data-access process. The draft delegated act should be improved having in mind that sharing data (including sensitive information) with any third party will always risk causing vulnerabilities both (1) to VLOPs and VLOSEs and the systems and processes they have put in place to protect such data, and (2) to the protection of confidential information, including user information and trade secrets. Further support for Digital Services Coordinators (DSCs) and reliance on the expertise of VLOPs and VLOSEs – referred to as 'data providers' in this context – are needed.

The Association hopes that the identified gaps will be filled, so that the Commission provides a robust and secure data-access framework. Below you will find CCIA Europe's three key recommendations to make data access for researchers as safe as possible for users and companies:

I. Set out appropriate requirements for the vetting process of researchers
II. Reinforce safeguards throughout the data-access application
III. Ensure secure and workable data-access modalities

[1] 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 here.
[2] CCIA Europe, DSA: Preserving fundamental rights when authorities and researchers access data, 3 October 2023, available here.

I. Set out appropriate requirements for the vetting process of researchers

As it stands, the draft delegated act on data access' main gap is the lack of a harmonised vetting process for researchers. This is largely left to the discretion of DSCs, which may result in a lack of parity for researchers and platforms subject to the regime. Because of this lack of guidance, several potential issues around the vetting of researchers are not – or are insufficiently – tackled in this draft delegated act.

The first issue that is not addressed by the delegated act is the role of VLOPs and VLOSEs, in the research vetting process. They should be permitted an opportunity to submit relevant documentation and information on applicant researchers as part of the DSC's vetting process. VLOPs and VLOSEs should also be permitted to review and comment on information and documentation provided as part of a researcher's application – not only a summary. Failure to allow for such participation by providers in a process which affords third parties unprecedented access to data relating to their businesses would set a dangerous precedent of an unbalanced process.

Second, the draft delegated act does not sufficiently guard against the potential misuse of the data access process by researchers with malicious intent and/or from a country outside of the European Union. Article 8(2)(c) only mentions "confirmation of affiliation" as one of the documents to include in the data-access application. The delegated act should be more granular in that regard and should require that researchers be employed by or enrolled at an organisation based in the EU. Such affiliation would also help to hold the research organisation, rather than the individual researcher, accountable, and liable in case of data misuse.

Third, the vetting process does not sufficiently ensure that researchers can and will protect sensitive data, including private information of users and businesses' trade secrets. The ability of researchers to protect this data should be thoroughly scrutinised by DSCs in the vetting process, with input from data providers. The possibility that bad actors will target researchers with hacking attempts or intimidation cannot be disregarded. This risk should be mitigated in the vetting process of researchers, as well as later in the data-access application and modalities.

Finally, the draft delegated act does not establish sufficient safeguards or liability regimes in the event something goes wrong. Article 40(10) of the DSA mentions the possibility for a DSC to terminate access and remove the vetted researcher status. More detailed rules should be included in the delegated act. However, in the absence of clarity, it should be assumed that researchers or the organisation they are affiliated with, will assume liability in case of external data misuse.

Indeed, the draft is silent about data breaches or researchers not respecting the conditions set out by the DSC to access data, which could give rise to very significant consequences given the wide range of data which will be accessible as listed in Recital 12 of the draft delegated act. The delegated act should expressly prohibit researchers from using data in a manner not authorised in a reasoned request, and specify legal consequences for researchers who fail to safeguard the data. Providing harmonised rules for these cases is vital for all involved parties to have legal certainty and trust in the data-access system.

A mechanism should also be created to permit data providers to apply to DSCs to review and remove a researcher's vetted researcher status in circumstances where they identify that a researcher may no longer meet the criteria set out in Article 40(8) of the DSA.

II. Reinforce safeguards throughout the data-access application

In the data-access application process, safeguards to protect businesses' trade secrets and the privacy of users should be reinforced. The draft delegated act itself rightly identifies these necessary objectives. However, in its current form, the draft delegated act insufficiently considers data protection and collaboration with VLOPs/VLOSEs.

Firstly, Article 6(4) of the draft delegated act introduces a transparency requirement that mandates platforms publish an "overview of the data inventory of their services." Making this overview public can have serious data protection and security implications. Besides, this new requirement goes beyond the scope of setting technical conditions for data access. Considering the dynamic nature of platforms and the evolving nature of data types, maintaining such an inventory would place an undue burden on platforms, particularly when researcher interest is limited, and could compromise the security of the data. To address this, the requirement should be removed.

Further, the examples of 'data' that may be the subject of a data-access request provided in Recital 12 of the draft delegated act are overly broad and do not align with the approach taken by the DSA. For example, Recital 12 of the draft delegated act includes a reference to: "data related to prices, quantities and characteristics of goods or services provided by the data provider". This should be revised reflect to the more limited approach adopted in Recitals 97 and 98 of the DSA, which limits data to metrics: "Data access requests could cover, for example, the number of views or, where relevant, other types of access to content by recipients of the service prior to its removal by the providers of very large online platforms or of very large online search engines".

Any examples of data provided in the delegated act should align with the approach taken in the DSA, to ensure that the delegated act does not stray beyond its implementing statute. Furthermore, in order to fulfil reasoned requests, data providers should not be required to generate data that they do not hold. Reasoned requests should be confined to existing data.

Moreover, the draft delegated act gives insufficient consideration to the rights and interests of users and data subjects, despite the many references to the General Data Protection Regulation.[3] To mitigate that concern, DSCs should be explicitly required to weigh these rights when determining access conditions and amendment requests. Overall, the approach and safeguards of the draft delegated act should include anonymisation of data, data aggregation, secure processing environments, and confidentiality agreements. Adopting such safeguards in the draft delegated act would strengthen protections for user data and privacy across the data-access process. Further, data providers should be given the opportunity to opine on the safeguards that might be appropriate for the data being shared pursuant to a data-access request. In the same vein, Article 13 of the draft delegated act

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), available here.

should require mediators in charge of dispute settlement over amendment requests to have data protection and users' privacy as one of their main objectives. The draft delegated act should also clarify the articulation of researchers' data access with other legal frameworks, such as the NIS 2 Directive[4] or the Trade Secrets Directive[5].

The lack of specific requirements for researcher capacity to protect data is also concerning. While DSA Article 40(8)(d) mandates researchers to demonstrate their capacity to meet data security requirements, this cannot be fully addressed at the application stage. Researchers should be required to submit comprehensive technical documentation before and after the DSC has formulated a preliminary reasoned request.

Furthermore, a 'commitment letter' is insufficient. Instead, more detailed, technical information and documentation evidencing the researcher's ability to protect data should be shared with VLOPs and VLOSEs. VLOPs and VLOSEs should be permitted to provide their views and feedback to DSCs before a reasoned request is formulated. Vetted researchers will be able to access data on VLOPs and VLOSEs' techniques used to proactively detect bad actors or illegal content. This type of information cannot be disclosed without sufficient safeguards – including safeguards relating to the potential publication by researchers of any statements relating to such data.

On the procedural level, several elements of the draft delegated act seem misguided. The very limited time given to DSCs to review data-access applications – five working days – in Article 7 of the draft delegated act is too short to allow DSCs to review the application properly. Forcing DSCs to issue decisions within five working days risks undermining trust in the data-access regime. In addition, the DSC should be able to ask for further information from the vetted researchers beyond these five days.

Another problematic issue with the current proposed approach is that VLOPs and VLOSEs can only access a summary of the researcher's data-access application in Article 10 of the draft delegated act. This excludes important information such as the researcher's funding sources, independence, conflicts of interest, and ability to comply with data protection standards. VLOPs and VLOSEs need full transparency into these aspects to assess risks, particularly regarding potential conflicts of interest and data security requirements and should be given access to all the documents provided by a researcher, rather than merely a summary. VLOPs and VLOSEs should explicitly be given an opportunity to comment on this information.

Similarly, access should only be granted to individual vetted researchers to enhance security, as opposed to Article 10(2) of the draft delegated act suggesting that entire organisations may access data. The final delegated act should also make it clear that, while research resulting from provided data sets may be made public, the data provided pursuant to a reasoned request must not be published by vetted researchers without the explicit consent of the relevant VLOP or VLOSE.

[4] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), available here.
[5] Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, available here.

The final delegated act should also provide criteria on how a "reasonable period" for data providers providing data should be defined or set by a DSC. This guidance is key to ensuring that VLOPs and VLOSEs are given enough time to comply with vetted requests and to ensure that all DSCs adopt a consistent approach. Further, the final delegated act should include provisions to pause the 'reasonable period' for providing data in circumstances where (i) a VLOP or VLOSE has issued an amendment request, or (ii) a mediation has been instigated under the dispute resolution mechanism provisions.

Finally, transparency regarding consulted experts and supervisory authorities is critical. Article 14 of the draft delegated act enables DSCs to consult experts, yet there is no requirement to disclose these consultations to data providers. To ensure informed decision-making, DSCs should disclose any expert attestations, opinions, or supervisory authority recommendations to data providers, allowing them to consider any amendments and mediation. VLOPs and VLOSEs should also be permitted to review documentation provided by potential experts and provide feedback during the selection process of experts. The final delegated act should also include criteria setting out how the experts are vetted and selected. For the avoidance of doubt, this should not prevent DSCs from taking legal advice from specialist external counsel and benefitting from relevant and applicable legal privilege.

III. Ensure secure and workable data-access modalities

To facilitate secure and practical data access, clear and feasible requirements must be established within the draft delegated act. Currently, several provisions create ambiguity and could place unnecessary burdens on data providers.

There are unworkable procedures regarding access modalities in the draft act, particularly the lack of initial consultation with data providers about secure access environments. Many providers have established secure access setups with specific, built-in tools and features. The current draft risks complicating these setups by not considering these environments in advance, which would likely lead to frequent requests for amendments and mediations with each reasoned request.

The process will work better for all parties – researchers included – if data providers can provide input before the DSC decides on modalities. The act should establish a proactive consultation process between DSCs and data providers regarding access modalities. This would enable providers to discuss their secure access environments and the restrictions on data storage, deletion, and analytics tools inherent to those environments before the DSC issues any reasoned requests. This proactive approach would streamline applications, reduce case-by-case amendment requests, and provide assurance to VLOPs and VLOSEs that their data, services, and user information remain protected. Additionally, this transparency would inform researchers early on about the security measures required for different access modalities, enabling them to tailor their applications accordingly.

Moreover, access restrictions within secure processing environments are essential. The draft currently prohibits providers from limiting researchers' use of analytical tools or enforcing data storage and deletion requirements, which is incompatible with maintaining a secure processing environment. For these environments to function securely, restrictions on allowed actions, software, and data governance processes are necessary. Failing to set such restrictions could also result in legal uncertainty around compliance with privacy

regulations if accessed data is combined with external sources within a provider's secure environment. For this reason, the final delegated act should permit VLOPs and VLOSEs to place appropriate limits and restrictions on the use of analytical tools and impose any archiving, storage, refresh and deletion requirements necessary to keep data secure and comply with applicable data privacy legislation.

Provisions concerning analytical tools and data access also require clarification. Draft Article 15(4) permits providers to restrict researchers' use of analytical tools if specified in a reasoned request, yet Article 15(3) broadly prohibits providers from imposing "archiving, storage, refresh, and deletion requirements." The draft delegated act should instead permit data providers to determine the appropriate access modalities whenever the data is of such a nature as to warrant sharing it in a secure processing environment (such as personal user data or confidential platform information).

Finally, the draft delegated act provides insufficient time for notifying DSCs of researchers' data access or termination. Draft Article 15(1) requires data providers to inform the DSC within 24 hours of granting or revoking researcher access to data. This timeframe is overly restrictive and could be challenging to meet consistently. To address this, the notification period should be extended to at least three business days, accommodating operational practicalities.

Conclusion

The European Commission has a unique opportunity to ensure that this unprecedented framework providing data access to researchers strikes the necessary balance with the fundamental rights of both users and businesses. That is why CCIA Europe hopes that its feedback supports the improvement of the draft delegated act on data access. The Association and its Members remain available to further discuss this feedback to make sure that data access is workable and safe for all.

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.

Visit ccianet.eu, x.com/CCIAeurope, or linkedin.com/showcase/cciaeurope to learn more.

For more information, please contact:

CCIA Europe's Head of Communications, Kasper Peters: kpeters@ccianet.org