weizenbaum
POLICY PAPER

SEPTEMBER 2025
14

LK Seiling, Clara Iglesias Keller, Jakob Ohme,
Ulrike Klinger, Claes de Vreese

Data Access for Researchers under the Digital Services Act: From Policy to Practice

ABOUT THE AUTHORS

LK Seiling \\ Weizenbaum Institute, Berlin
Clara Iglesias Keller \\ Weizenbaum Institute, Berlin
Jakob Ohme \\ Weizenbaum Institute, Berlin
Ulrike Klinger \\ University of Amsterdam
Claes de Vreese \\ University of Amsterdam

Contact: lukas.seiling@weizenbaum-institut.de

ABOUT THIS PAPER

Weizenbaum Policy Papers provide scientifically grounded statements, position papers, and briefings on current political topics and decision-making processes.

This report draws on information and experience gathered from a transnational network of researchers, civil society, regulatory agencies, political representatives, and platforms built by the DSA 40 Data Access Collaboratory, led by some of the authors of this paper. Since early 2024, the joint project funded by Mercator Stiftung has been monitoring and engaging in the legislation's implementation process to evaluate to what extent scientists and non-profit organisations receive data access for the study of systemic risks.

ABOUT THE WEIZENBAUM INSTITUTE

The Weizenbaum Institute is a joint project funded by the German Federal Ministry of Research, Technology and Space (BMFTR) and the State of Berlin. It conducts interdisciplinary and basic research on the digital transformation of society and provides evidence- and value-based options for action in order to shape digitalization in a sustainable, self-determined and responsible manner.

Weizenbaum Policy Paper

Data Access for Researchers under the Digital Services Act: From Policy to Practice

LK Seiling, Clara Iglesias Keller, Jakob Ohme, Ulrike Klinger, Claes de Vreese

Abstract

As digital platforms play an increasingly prominent role in societies around the globe, calls from policymakers, civil society, and the public for transparency, accountability and evidence-based regulation of these digital services have become louder and more urgent. Independent research seeking to provide such empirical evidence has either taken place in a legal gray zone, running the risk of legal retaliation, or depended on close collaboration with platforms. The Digital Services Act (DSA), adopted in 2022 and in force since 2024, promises to change this dynamic by clearly outlining under which conditions platforms must grant data access to researchers. The recently adopted Delegated Act on data access (DA) provided more detail on the implementation of this new right to data access for researchers. This paper provides an overview of researchers' initial practical experience with access to publicly available data based on Art. 40(12) DSA as well as an in-depth description of procedure for access as set out in Art. 40(4) DSA, thereby comprehensively characterising the data access options outlined in the DSA and DA. We outline key provisions and their underlying rationales to provide an overview of the goals, procedures and limits of DSA-based data access, as well as an account of external factors likely to weigh in its realisation. The goal is to offer a valuable point of reference for the European as well as global community of researchers considering applications under the DSA, as well as other stakeholders aiming to understand or support the development of robust data access frameworks.

Contents

Executive Summary

The European Union's Digital Services Act (DSA) aims to increase transparency and accountability for Very Large Online Platforms and Search Engines (VLOPSEs) through a variety of measures and obligations. This policy paper focuses on the **obligation of platforms to provide data access to researchers as established in Art. 40 DSA**, a significant shift from previous, non-regulated access regimes, and the tensions and challenges resulting from its implementation, operating within existing power structures between platforms and governments. A central element of the VLOP-specific obligations is the concept of **systemic risk**. It also serves as the foundation for data access requests under Article 40, as the requested data must be used for research that contributes to the understanding, identification, detection, or mitigation of such risks **in the European Union**. While researchers also need to meet other requirements (such as independence of commercial interests), the purpose limitation is the only factor that geographically restricts the scope of the research. This means that while the research itself is geographically limited in scope, access can in principle be granted to all researchers that meet the specified vetting criteria, independent of their location.

Two modes of data access

Art. 40 DSA outlines two distinct modes of data access for researchers:

Access to data that is publicly accessible (Article 40, paragraph 12): This provision requires platforms to provide (if possible real-time) access to data that is publicly available on their online interfaces. This mode holds great potential for risk monitoring and knowledge creation, as it allows researchers to access data without undue delay. However, in the first year since initial availability researchers have experienced practical obstacles, including inconsistent application forms, platforms stalling requests, and data quality issues.

Privileged access to data (Article 40, paragraph 4): This broader provision provides a more general access to data. This includes data that may be publicly available but not provided by platforms as well as clearly non-public data such as personalized recommendation histories or internal documentation. Unlike access based on Art. 40(12), for this type of access researchers are not vetted and authorised by the platforms but instead by national Digital Service Coordinators (DSCs), which results in many responsibilities focused on the Irish Coimisiún na Meán, as most VLOPs reside in Ireland. The recently adopted delegated act on data access has specified this authorisation procedure. Drawing on an analysis of the delegated act as well as practical experiences from pilot studies, we outline specific challenges related to this kind of access: researchers need to request specific data but lack the internal knowledge of what data platforms collect and are additionally responsible for implementing strict legal, technical and organisation measures to mitigate risks to data security, data protection, and confidentiality.

Conditions for the successful realisation of data access

Based on the empirical and theoretical insights, we argue that realising effective data access needs more than just a legal framework; it requires

well-resourced, independent, and fair intermediaries: National governments must support DSCs through proper funding and ensure their independence and international coordination, which could serve to remedy potential challenges introduced by the bottleneck position of Ireland's Coimisiún na Meán.

platform cooperation: While compliance is the baseline, meaningful data access requires active cooperation and a presumption of good faith from platforms. Unfortunately, a lack of cooperation, driven by geopolitical and economic tensions, is likely to continue to pose a considerable challenge to successful implementation.

robust public enforcement and institutional innovation: The European Commission needs to maintain a firm stance on enforcement to ensure the basic conditions for data access. Additionally, it could and should support the build-out of the data access framework through soft law instruments and encouraging voluntary agreements, like codes of conduct, to address emerging issues and foster new institutional solutions.

researcher organisation: Researchers should engage in "strategic boundary work" to actively shape the data access framework by clarifying legal interpretations and establishing best practices. This includes developing resilient, independent infrastructure to handle large-scale data and ensure data quality, as well as a need for collaborative efforts to pool resources and share information.

adequate funding: Research budgets should reflect the substantial financial and institutional commitment required to establish a broad research landscape and infrastructure that allows diverse and responsible knowledge creation on systemic risks and ensure that high costs do not jeopardise the quality and integrity of scientific progress and innovation.

1 Introduction

Article 40 of the European Digital Services Act (DSA) provides a crucial tool for researchers interested in studying socio-political dynamics in online spaces: it obliges Very Large Online Platforms or Search Engines (VLOPSEs) to provide access to data.

In July 2025, the European Commission adopted the Delegated Act (DA) on data access, which had been eagerly awaited by researchers, as it specifies important processes, caveats and rules for researcher access to non-publicly available platform data, a process that had not yet been clearly regulated. The resulting legal framework represents a landmark regulatory effort to reshape the relationship between digital platforms and the research community. By creating formal procedures for data access, it transforms previous dynamics, which often left researchers dependent on platforms' goodwill or informal contacts, and establishes a transparent, standardised process for accessing data. This shift holds significant potential to advance public knowledge, not only on platform effects but also on the broader risks posed to individual rights and the robustness of European democracies.

Nonetheless, realizing the promise of transparency under Art. 40 DSA is complicated by a number of aspects within and beyond its legal framework. First, as with other provisions of the DSA, the effectiveness of data access will largely depend on how key legal categories are interpreted, notably the idea of systemic risk. In this realm, platforms remain strategically positioned to drive narratives, create obstacles or even limit access to data. Platform politics are still politics, and as such, these companies' have mixed incentives to cooperate, and are often subject to geoeconomic interests that go beyond the scope of the DSA.

Against this background, this policy paper seeks to provide researchers with a comprehensive overview of the background, procedures and challenges involved in leveraging Art. 40 DSA for the creation of public knowledge about platform operations. It highlights key provisions of both the DSA and the DA, exploring legal and practical challenges to data access, while also addressing the potential pathways for mitigating these barriers and maximising the provision's impact.

In Section 1, we provide a brief overview of the Digital Services Act, particularly with regard to the regulatory shift towards holding digital platforms accountable for their business models. One of the pillars of this approach is the implementation of transparency mechanisms, such as the one in Article 40. We will also explore the casting of systemic risk as both the core of reporting obligations and standard for the applicability of other provisions, especially Art. 40 DSA.

In Section 2, we zoom in on Art. 40 DSA and the DA to provide a detailed account of its scope, addressing key questions for researchers to engage with the provision, such as: What kinds of data can researchers request? What procedures are involved in securing access? How do platform obligations differ depending on the nature of the data? And what frictions have emerged in the first year of implementation?

In Section 3, we zoom out to account for specific factors that are likely to weigh on the realisation of research data access. We explore how institutional design, platform cooperation, enforcement practices, researcher agency, infrastructure and funding all interact with—and at times undermine—the promise of Art. 40 DSA. By examining these structural, political and operational dimensions, we show that realizing an accessible and sustainable data access framework requires far more than legal entitlement: it demands coordinated, well-supported

2 Regulatory Background: the Digital Services Act

The DSA has been in force since November 2022, with an overarching regulatory approach aimed at holding digital platforms accountable. As a cornerstone of European digital policy, the DSA represents a shift from the previous E-commerce Directive[1], which established that platforms can be held liable for damage caused by user-generated content if they fail to remove it upon notification. While retaining this possibility, the DSA expands the horizon of platform accountability. Beyond the duty to repair damage after it occurs, it seeks to infuse platforms' everyday operations with obligations aligned with the procedural principles of the rule of law, like due process, contestation and the ultimate goal behind Article 40: transparency.

Due to its comprehensive approach, the DSA has been often framed as a "shift from liability to responsibility"[2] or "from liability to duty"[3], in a regulatory reach over major technology corporations that other countries tried, but failed, to establish—arguably, due to lacking sufficient political leverage against strong lobbying[4]. Nevertheless, the extent to which the new obligations could potentially address the concentration of power among few major tech firms in Europe is an object of skepticism in specialised literature. Natali Helberger, for instance, argues that DSA's core approach towards improving procedural legitimacy validates, rather than challenges, fundamental aspects of platforms' surveillance capitalism-based business models.[5] Other authors have scrutinised the DSA's reliance on platforms to assess and mitigate *systemic risks*, a concept that also conditions access to data (a point we will further develop shortly). Critiques here range from the vagueness of this legal category to the fact that companies will have a key role in interpreting and implementing the provision, in a

1 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market ('Directive on Electronic Commerce'), CONSIL, EP, 178 OJ L (2000). http://data.europa.eu/eli/dir/2000/31/oj/eng

2 Frosio, G. (2017). Why keep a dog and bark yourself? From intermediary liability to responsibility. International Journal of Law and Information Technology, 1–33. https://doi.org/10.1093/ijlit/eax021

3 Mac Síthigh, D. (2020). The road to responsibilities: new attitudes towards Internet intermediaries, Information & Communications Technology Law, v. 29, n. 1, p. 1-21.

4 Regulation of Digital Platforms in Brazil on the Verge of Succumbing to Big Tech Interests - Latinoamérica 21.

5 Helberger, N. (2020). The Political Power of Platforms: How Current Attempts to Regulate Misinformation Amplify Opinion Power. Digital Journalism, 8(6), 842–854. https://doi.org/10.1080/21670811.2020.1773888

continuation of regulatory approaches that tend to maximise "corporate freedoms and profitability".[6]

The DSA is characterised by this tension, implementing (ideally significant) means for accountability within the borders of pre-established power arrangements. This dynamic is particularly evident when we analyse Article 40, whose core purpose is to grant supervision authorities and researchers access to the data necessary for assessing compliance with the regulation.

Despite its potential, the extent to which Article 40 succeeds in promoting access to reliable and useful data will depend on a constellation of factors, including the applicable legal provisions (DSA and Delegated Act), the supervision authorities' enforcement capacities, and the ongoing geopolitical power struggles between platforms and governments.

DSA-based data access and the promise of platform transparency

Platforms' obligations provided by the DSA apply asymmetrically, meaning that the regulatory burden over implementing accountability procedures is highest for the platforms with the furthest reach. Specifically, Art. 40 DSA applies to Very Large Online Platforms and Search Engines (VLOPSEs) with over 45 million "recipients of the service" in the EU.[7]

Such platform companies increasingly influence social and political interactions of billions of users around the globe, leveraging information and attention fluxes online according to their opaque commercial criteria. Until now, access to platform data (e.g. large-scale user behaviour[8]) depended on platforms' goodwill or personal relationships. With the DSA and the Delegated Act in force, researchers have an institutional channel to access platform data, whether publicly available or not, as long as they meet the relevant criteria set out in the DSA.

Beyond empowering regulators and researchers to scrutinise and challenge corporate governance mechanisms, Art. 40 DSA also serves broader societal interests, including facilitating the production of knowledge on digital platforms' technical architectures as well as the economic, social and political relationships they reflect and reinforce. This, in turn, supports not only the efficacy of the DSA but the development of future evidence-based public policy in numerous fields, including consumer law, minorities protection and technology regulation.

---

6 Griffin, R. (2025). Governing platforms through corporate risk management: The politics of systemic risk in the Digital Services Act. European Law Open, 1–31. https://doi.org/10.1017/elo.2025.17

7 Art. 33 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), 277 OJ L (2022). http://data.europa.eu/eli/reg/2022/2065/oj/eng

8 Guess, A. M., Malhotra, N., Pan, J., Barberá, P., Allcott, H., Brown, T., Crespo-Tenorio, A., Dimmery, D., Freelon, D., Gentzkow, M., González-Bailón, S., Kennedy, E., Kim, Y. M., Lazer, D., Moehler, D., Nyhan, B., Rivera, C. V., Settle, J., Thomas, D. R., … Tucker, J. A. (2023). How do social media feed algorithms affect attitudes and behavior in an election campaign? Science, 381(6656), 398–404. https://doi.org/10.1126/science.abp9364

In practice, the process of requesting and obtaining data from digital platforms has proven to be problematic, unreliable, and not scalable. Throughout this paper, we highlight key potential points of dispute, in- and outside the legal scope designed in Art. 40 DSA and the Delegated Act, the first one being the vague legal category of *systemic risks*.

Systemic risk as the foundation of DSA-based data access

Systemic risks lie at the core of the obligations specific to VLOPSEs, including the research data access provisions in Art. 40 DSA. Specifically, the data accessed must be used "solely for performing research that contributes to the detection, identification and understanding of systemic risks in the Union, as set out pursuant to Article 34(1)" or "for the assessment of the adequacy, efficiency and impacts of the risk mitigation measures pursuant to Article 35" (see Table 1).

Articles 34 and 35 of the DSA provide that VLOPSEs must assess and mitigate systemic risks "stemming from the design or functioning of their services and its related systems [...] or from the use made of their services",[9] with Art. 37 DSA additionally requiring these procedures to be audited by external auditors. Art. 34(1) DSA points at what types of systemic risks are of initial concern to the regulator: the dissemination of illegal content; actual or foreseeable negative effects on fundamental rights, civic discourse, electoral processes and public security; gender-based violence; the protection of public health and minors; as well as negative effects on people's physical and mental well-being. These risks constitute the minimum set[10] that must be included in the reports, and is open for conceptual and practical expansion. Art. 35(1) similarly only includes a list of exemplary mitigation measures, touching on both the platforms' systems as well as the underlying governance structures.[11]

These risk-related duties are centered on the idea that platforms are uniquely positioned and responsible for making sure that their services do not contribute to the spread of the online harms associated with the risks categories described. The same underlying rationale also inspires other DSA provisions, such as the "Crisis Response Mechanism" provided in Article 36, according to which, upon recommendation of the Board, VLOPSEs must take immediate action against sensitive threats, or the data access provisions Art. 40 DSA.[12] While some of these provisions reference classical conceptions of risk that can be unambiguously measured and

9 The fact that risks can stem both from the design or functioning of the platform's services and their use shows that platforms are not the sole cause of risk. As popular content distribution services they can be understood as highly connected nodes within socio-technical networks through which information flows. Thus, while they can create and or contribute to risks, they are also in a unique position to reveal risks that originate outside their services.

10 Kaesling, K. (2023). Art 34. Risikobewertung. In F. Hofmann, B. Raue, M. Dregelies, & K. Grisse, Digital Services Act: Gesetz über digitale Dienste (1. Auflage). Nomos, p. 560.

11 Kaesling, K. (2023). Art 35. Risikominderung. In F. Hofmann, B. Raue, M. Dregelies, & K. Grisse, Digital Services Act: Gesetz über digitale Dienste (1. Auflage). Nomos., p. 583.

12 VLOPSEs have to provide the data necessary for monitoring compliance (with their risk management obligations) to regulatory and enforcement bodies (Art. 40(1-2) DSA) or explain their algorithmic systems to them (Art. 40(3) DSA). Art. 40(4-12) DSA covers researcher data access and Art. 40(13) provides the EC with the option to further specify researcher data access through delegated acts.

mitigated[13], obligations such as the crisis response mechanism point towards a notion of risk as more difficult to foresee, capture and adequately prepare for or respond to,[14] arguably requiring a different set of responses.[15]

Thus, while platforms are responsible for internal risk management, the concrete understanding of what constitutes systemic risks relies just as much on researchers and the supervising Digital Service Coordinators (DSCs) as they shape the development of this legal category through access requests under this provision. Thus, engagement with the systemic risk category resembles a feedback loop, where the initial understanding is iteratively explored and built upon based on scientific theory and evidence. While this approach allows for a certain flexibility regarding the interpretation of systemic risk, it also requires all data access applications to make reference to systemic risk as defined by the DSA.

3 Zooming In: How to Access Data under Article 40 DSA?

Art. 40 DSA differentiates researcher data access based on its scope:

- paragraph 12 obliges platforms to provide researchers with access to data that is "publicly accessible in their online interface"
- paragraph 4 is broader, establishing a more general form of data access, effectively providing researchers access to non-public data.[16]

As Table 1 shows, while both kinds of access are conditioned on researchers meeting eligibility requirements and purpose limitations, they notably do not reference the researchers' location. Thus, in principle access to platform data — no matter if publicly available or not — is

13 Such realist conceptions of risk, which assume that risks objectively exist and can be quantified based on estimates for their probability of occurrence and a numerical value indicating the severity of a given risk, underlie classic risk management or governance frameworks. See for example ISO. (2018). Risk management—Guidelines (No. 31000:2018(E)). https://www.iso.org/standard/65694.html or IRGC. (2017). Introduction to the IRGC Risk Governance Framework, Revised Version. EPFL International Risk Governance CenterEPFL International Risk Governance Center. https://irgc.org/wp-content/uploads/2018/09/IRGC.-2017.-An-introduction-to-the-IRGC-Risk-Governance-Framework.-Revised-version..pdf

14 Indeed, systemic risks are often characterised as being temporally, factually and socially decoupled, and requiring effective cross-disciplinary collaboration to come up with adequate responses. See for example Renn, O., Laubichler, M., Lucas, K., Kröger, W., Schanze, J., Scholz, R. W., & Schweizer, P. (2022). Systemic Risks from Different Perspectives. Risk Analysis, 42(9), 1902–1920. https://doi.org/10.1111/risa.13657, or Helbing, D. (2013). Globally Networked Risks and How to Respond. Nature 497 (7447): 51–59. https://doi.org/10.1038/nature12047.

15 One potential policy tool to respond to systemic risks is planned adaptive governance, a multi-stakeholder approach to risk governance in which explicitly includes arrangements that are reviewed and updated in the face of uncertain or changing evidence. See also IRGC. (2018). Guidelines for the Governance of Systemic Risks. https://doi.org/10.5075/EPFL-IRGC-257279

16 Husovec has dubbed these different modes of access "public data access" and "privileged data access" respectively. See Husovec, M. (2024). General Risk Management. In Principles of the Digital Services Act. Oxford University Press.

to be granted to all researchers that meet the specified vetting criteria and *solely* conduct research on systemic risk inside the European Union.[17]

As such, while limiting the object of research to EU-related risks, DSA-based data access does not privilege European researchers and will likely foster international collaboration and thus have a beneficial impact on the amount of knowledge produced based on this provision. This sort of equal access additionally prevents the EU from creating a closed off research environment – a direct response to previous access conditions which disproportionately privileged US researchers, who have closer ties with US-based tech companies.

How does it work for publicly accessible data?

The DSA has been obligating VLOPSEs to provide access to publicly accessible data since February 2024. Though data access for commercial use has been a longstanding practice across platforms[18], the obligations introduced by the DSA were met with mixed responses: for example, TikTok introduced a dedicated research API[19], whereas Meta and X further limited the data available for research purposes.[20]

In order to be granted access, researchers currently have to complete platform-specific application forms or provide relevant information via email to be then vetted by the provider of the VLOPSE, or an appointed surrogate institution.[21] If the platform finds them to meet the eligibility requirements, they can start to access data through various modalities, ranging from graphical user interfaces, over APIs, secure processing environments, and dedicated datasets to permissioned scraping.[22]

---

17 While it seems contradictory to put forth a concept as broad and unbounded as systemic risk only to then strictly limit the purposes of data access to research on such risks within the European Union, there are ways to resolve this paradox: The geographical restriction keeps the provision from being construed as establishing extraterritorial or global access rights. At the same time, the openness of the systemic risk concept allows for a wide-lense approach to research which accommodates the incremental and non-linear reality of empirical and theoretical research.

18 Evans, P. C., & Basole, R. C. (2016). Revealing the API ecosystem and enterprise strategy via visual analytics. Communications of the ACM, 59(2), 26–28. https://doi.org/10.1145/2856447, Snodgrass, E., & Soon, W. (2019). API practices and paradigms: Exploring the protocological parameters of APIs as key facilitators of sociotechnical forms of exchange. First Monday. https://doi.org/10.5210/fm.v24i2.9553

19 Moon, M. (2023, February 21). TikTok opens data to US researchers in its bid to be more transparent. Engadget. https://www.engadget.com/tiktok-launches-research-api-140028148.html

20 Mehta, I. (2023, February 14). Twitter's restrictive API may leave researchers out in the cold. TechCrunch. https://techcrunch.com/2023/02/14/twitters-restrictive-api-may-leave-researchers-out-in-the-cold/, Gotfredsen, S. G., & Dowling, K. (2023, July 9). Meta Is Getting Rid of CrowdTangle—And Its Replacement Isn't as Transparent or Accessible. Columbia Journalism Review. Retrieved 1 September 2025, from https://www.cjr.org/tow_center/meta-is-getting-rid-of-crowdtangle.php

21 ICPSR has taken a related role in cooperation with Meta, see ICPSR. (2023, November 21). ICPSR to facilitate researcher access to Meta's API Products. https://www.icpsr.umich.edu/web/about/cms/5231

22 Giglietto, F., & Terenzi, M. (2024). PROMPT - The State of Social Media Research APIs & Tools in the Digital Service Act Era (No. ENO-PROMPT LC-02629302). https://drive.google.com/file/d/1htMFVxELz2hHPTCDARlWe2iqcWQsM6eQ/view, Hickey, C., Dowling, K., Navia, I., & Pershan, C. (2024). Public Data Access Programs: A First Look (p. 51). Mozilla Foundation. https://assets.mofoprod.net/network/documents/Public_Data_Access_Programs__A_First_Look.pdf

This mode of data access is promising, because it allows a wide range of researchers (if technically possible real-time) access to publicly available data without undue delay, which could contribute to decentral risk monitoring (meaning identification and detection) and other forms of knowledge creation. While researchers have gotten access to publicly available data from VLOPS such as X, TikTok, or Meta, the first year of researcher data access in practice has shed light on various obstacles that keep this promise from becoming reality:[23] The information required for access applications varies strongly between platforms, some of which is at most tangentially related to the requirements set out in Art. 40(8b-e).[24] Still, after successful submission of their application, some researchers have reported being rejected due to not residing in the EU. Others report being stalled by platforms, often involving a lengthy back and forth in which the platforms require researchers to progressively narrow the purposes of their research and scope of the data to be accessed.[25] And even after researchers have received data access, they still report issues with data quality[26], which they detected through scraping, the legal status of which is unclear.[27] These issues could be addressed through the development of codes of conduct between platforms and research organisations or through additional guidance on the implementation of Art. 40(12) DSA issued by the EC, which has thus far not been atop its list of priorities. Instead, it has been at work in a delegated act, specifying privileged data access as set out in Art. 40(4) DSA, which is supposed to allow researchers to literally and figuratively go beyond surface-level data access.

23 For another overview, see Mimizuka, K., Brown, M. A., Yang, K.-C., & Lukito, J. (2025). Post-Post-API Age: Studying Digital Platforms in Scant Data Access Times. arXiv. https://doi.org/10.48550/arXiv.2505.09877

24 The number of individual questions varies between 8 (Snap) and 55 (Meta). Some platforms limit those to information directly relevant to the access application, while others also require researchers to provide their phone number (Meta, Pinterest) or date of birth (Meta).

25 Jaursch, J., Ohme, J., & Klinger, U. (2024). Enabling Research with Publicly Accessible Platform Data: Early DSA Compliance Issues and Suggestions for Improvement. Weizenbaum Institute. https://doi.org/10.34669/WI.WPP/9

26 Darius, P. (2024, September 24). Researcher Data Access Under the DSA: Lessons from TikTok's API Issues During the 2024 European Elections | TechPolicy.Press. Tech Policy Press. https://techpolicy.press/-researcher-data-access-under-the-dsa-lessons-from-tiktoks-api-issues-during-the-2024-european-elections, Entrena-Serrano, C., Degeling, M., Romano, S., & Çetin, R. B. (2025). TikTok's Research API: Problems Without Explanations (Version 2). arXiv. https://doi.org/10.48550/ARXIV.2506.09746, Pearson, G. D. H., Silver, N. A., Robinson, J. Y., Azadi, M., Schillo, B. A., & Kreslake, J. M. (2024). Beyond the margin of error: A systematic and replicable audit of the TikTok research API. Information, Communication & Society, 1–19. https://doi.org/10.1080/1369118X.2024.2420032

27 For details see Leerssen, P., Heldt, A., & Kettemann, M. C. (2023). Scraping By?: Europe's law and policy on social media research access. In Strippel, C., Paasch-Colberg, S., Emmer, M. & Trebbe, J. (Eds.). Challenges and perspectives of hate speech research. Freie Universität Berlin. https://doi.org/10.48541/DCR.V12.24, and Brown, M. A., Gruen, A., Maldoff, G., Messing, S., Sanderson, Z., & Zimmer, M. (2024). Web Scraping for Research: Legal, Ethical, Institutional, and Scientific Considerations (No. arXiv:2410.23432). arXiv. https://doi.org/10.48550/arXiv.2410.23432

How does it work for data that is not publicly accessible?

Following a two-year period of preparation[28], the delegated act on data access was adopted in July 2025,[29] aiming to establish "reliable, consistent and uniform practices" around privileged data access, initially specified in paragraph 4 to 11 of Art. 40 DSA. While some of the criticisms researchers had with the initial draft remain unaddressed in the adopted regulation,[30] it defines the necessary conditions and outlines an elaborate systematic process (see Figure 2) meant to address the two fundamental questions at the heart of research data access: What data can be accessed? And how?

What data can be accessed?

Articulating an answer to the first question is inherently difficult due to the fact that data meant to be accessed via Art. 40(4) DSA is *not* publicly accessible. Here, it is helpful to distinguish between data that A) is accessible through other means but is currently not provided by the platform (like the media bytes related to pieces of content, content labels, visibility restrictions, search recommendations, or non-follower engagement) and B) cannot be accessed through such alternative means (like relationship networks, individual-level content exposure and engagement histories, personalised recommendations or even internal documents detailing governance decisions).[31] For category A), researchers could theoretically use access requests to demonstrate data accessibility to enforcement bodies, which in turn could compel platforms to make this data available under Art. 40(12) DSA. Category B) however is characterised by a fundamental information asymmetry, or what Goanta et al. (2025) call an inherent standoff problem: "Researchers need to request specific data but are not in a position to know all internal data collected, processed and stored by VLOPs, who, in turn, expect and demand data specificity for potential access".[32]

---

28 An initial call for evidence was launched in April 2023, the responses to which were combined into a draft delegated act (DDA) that was published in October 2024. Feedback was collected until December 2024. For a documentation of the full process, see European Commission. (2025). Public Consultations and Feedback for the Delegated Regulation on data access provided for in the Digital Services Act. European Commission - Have Your Say. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13817-Delegated-Regulation-on-data-access-provided-for-in-the-Digital-Services-Act_en

29 European Commission (2025). Commission adopts delegated act on data access under the Digital Services Act. https://digital-strategy.ec.europa.eu/en/news/commission-adopts-delegated-act-data-access-under-digital-services-act

30 Seiling, L., Ohme, J., Klinger, U. (2024): Response to the Consultation on the Delegated Regulation on Data Access provided for in the Digital Services Act (Weizenbaum Policy Paper # 11). Weizenbaum Institute, Berlin. https://doi.org/10.34669/WI.WPP/11

31 Art 8(6) the Draft Delegated Act required researchers to include "an explanation as to why the research project cannot be carried out with alternative existing means such as using data available through other sources". While this passage was cut in the adopted DA, the authors hope that the reader will appreciate the theoretic usefulness of this distinction.

32 Goanta, C., Zannettou, S., Kaushal, R., Kerkhof, J. van de, Bertaglia, T., Annabell, T., Gui, H., Spanakis, G., & Iamnitchi, A. (2025). The Great Data Standoff: Researchers vs. Platforms Under the Digital Services Act. arXiv. https://doi.org/10.48550/arXiv.2505.01122

The DA attempts to address this imbalance by imposing extensive transparency obligations onto VLOPSEs: they have to provide relevant information (such as codebooks, changelogs and architectural documentation)[33], as well as DSA data catalogues, an overview over the accessible data[34], to researchers. For the provision of these, platforms can draw on existing resources for access measures for other purposes (e.g. for advertising, content creation or third-party app development). However, the data catalogues should also disclose which data was used for risk identification and mitigation, as reported in their annual risk reports, providing the foundation for researchers to understand, assess, replicate and build on the reports, as well as relevant methods and data. Adhering to the procedural approach taken by the DSA, the data included in the catalogues will also have to be regularly updated to account for evolving understanding of systemic risk and application of corresponding mitigation measures.[35] This suggests that data catalogues are inherently dynamic, expanding over time in response to researchers' data access requests and the evolving identification of risks and mitigation strategies. Thus, in principle, vetted researchers are free to request any kind of data in their access application – which comes with a set of challenges discussed below.

How can data be accessed?

The DSA's access regime requires the involved parties to specify request-specific access modalities, describing which legal permissions, organizational requirements and technical methods are put in place to enable secure and responsible data access. Generally, the access modalities must be proportionate to the risks posed to users' data protection and to the platforms' security and trade secrets[36]—with additional consideration for safeguards[37] in the case of data transfer to third countries[38] or international organisations. Importantly, by default researchers can freely handle the accessed data, unless limitations on data management and analysis are specified.[39]

Notwithstanding potential organisational or legal access conditions, Rec. 17 DA names two modes of data access: data transfer, where the data is transmitted onto a system maintained by the researcher, and secure processing environments (SPEs),[40] where data is stored and

33 Rec. 26 and Art. 15(2) DA.

34 Rec. 7-9 and Art. 6 DA.

35 Rec. 8 DA.

36 Specifically, the Art. 9(4) DA mentions data protection impact assessments as well as technical and organisational measures in case personal data is processed, but also network security measures, encryption, access control mechanisms, backup policies, data storage period, data destruction plans, data integrity mechanisms, internal review processes, restrictions of access rights and information sharing, contractual clauses (e.g. non-disclosure agreements, data agreements, other types of written statements), or training on data security and personal data protection more generally to be considered.

37 Rec. 17 & Art. 10(3) DA.

38 Countries the EU has deemed to not provide an adequate level of data protection. For more information see European Commission (2025). Adequacy decisions. https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

39 Art. 15(3) DA.

40 The requirements for the provision of secure processing environments are set out in Art. 9 DA.

accessed on specialised systems maintained by the platform or third party. However, it also explicitly includes "other access modalities to be set up or facilitated by the data provider", which means that other modes of data access, in principle, are possible under the DSA's data access regime. This could include a variety of researcher testbeds allowing for experimentation with simulated or real data,[41] or the consent-based linkage of platform and survey data[42]—which could greatly further knowledge generation by facilitating on-platform data collection instead of off-platform data processing.[43] Still, while researchers can make suggestions and platforms may request amendments, it ultimately is the responsibility of the supervisory authorities to determine the appropriate access modalities based on submitted applications for data access, as shown in the next section.

How does the data access process[44] work?

To evaluate access applications and decide the conditions for data access, DSA and DA put forth a process with predefined steps and timeframes (depicted in Figure 2), involving researchers, platforms and, centrally, the designated intermediaries: the Digital Service Coordinators (DSCs).[45] Key output of this process is a reasoned request for data access[46] (RR), formulated by the DSC of establishment (DSC-E), upon the receipt of which platforms should provide data access to researchers.

The RR, and any changes made to it during the procedure, will be published by the DSC-E on the DSA data access portal.[47] With its establishment, the European Commission (EC) aims to ensure harmonisation and increase efficiency by providing standardised application

41 Arntzen, S., Wilcox, Z., Lee, N., Hadfield, C., & Rae, J. (2019). Testing Innovation in the Real World: Real-world testbeds. Nesta. https://media.nesta.org.uk/documents/Testing_innovation_in_the_real_world.pdf

42 In cooperation with the Center for Open Science Meta has offered such data access part of a pilot programme (see cos.io/meta), similarly the DSA data access portal seems to foresee such access requests as it includes the question "Do you foresee that the data requested will be combined with other datasets?"

43 See also Seiling, L., Klinger, U., & Ohme, J. (2024). Non-Public Data Access for Researchers: Challenges in the Draft Delegated Act of the Digital Services Act. Tech Policy Press. https://www.techpolicy.press/non-public-data-access-for-researchers-challenges-in-the-draft-delegated-act-of-the-digital-services-act/

44 The authors are using the DA's terminology here, acknowledging that it is slightly misleading, given that the actual process of researchers accessing and working with the data is a consequence resulting from this 'data access process'. Thus, a more fitting title for the process described in the following would be "access authorisation procedure".

45 Following Art. 49 DSA, all EU member states have to designate a competent authority responsible for the supervision and enforcement of the obligations introduced under this legislation, esp. With regard to smaller platforms (for an overview, see https://digital-strategy.ec.europa.eu/en/policies/dsa-dscs#1720699867912-1). While EC takes over the role of supervision and enforcement in the context of data access, these Digital Service Coordinators (DSCs) still take a central role during the vetting of access applications. Their role differs with regard to the location of the VLOPSE from which data is requested: DSCs of (platform) establishment (DSC-Es) negotiate with the platforms. DSCs of (research organisation) member state (DSC-Ms) can support this process by providing expertise and by taking care of the initial application vetting.

46 Art. 10 DA specifies the contents of a RR, requiring start and end dates of access, the determined access modalities, and a summary of the researcher's access application.

47 European Commission (2025). DSA Data Access Portal. https://data-access.dsa.ec.europa.eu/home

templates for researchers, and a shared infrastructure for information exchange and documentation of the access process.

In broad terms, this process consists of up to four consecutive phases, the last three of which are shown in Figure 2, with the third and fourth phases triggered only upon request by the platform targeted by the access application:

1. Formulation and submission of the access application by the researcher
2. Application vetting and initial formulation of the RR *(max. 80 working days) by the DSC*
3. Amendment procedures for the RR *(max. 30 days)*
4. Mediation procedures *(max. 65 working days)*

Importantly, the DSC-E remains authoritative during the entire process: it has the final say on the content of a RR and the degree to which it engages with platform requests. Researchers on the other hand only play a comparably minor role in the process, starting it by submitting their access application. Considering that each phase is assigned a maximum duration, DSA and DA set the time limit of any data access process at 175 working days. This upper bound, while at worst still putting close to nine months between a researcher's application and access to data, provides researchers with a dependable timeframe to plan research projects or funding applications. It also hinders platforms from prolonging procedures indefinitely. Still, in order to guarantee timely processing, DSCs have to establish procedures for the swift handling of access applications, amendment requests and mediation requests.

Formulation and submission of the access application

The data access process starts with the principal researcher, the primary point of contact for all further communications, submitting an application for data access through the DSA data access portal,[48] which requires both the researcher and their institutions to be registered in the EC's systems.[49] Additionally, all other applicant researchers can be added, and all researchers will have to provide evidence of their affiliation to a research organisation of affiliation,[50] their independence from commercial interests,[51] and a commitment to making

48 The specific configuration of questions and response options will likely be subject to change before and after the first access applications can be submitted. Currently, for example, access applications can only be associated with a single systemic risk and cannot be easily duplicated, which might impede cross-platform research (although the form does already give researchers the chance to indicate other applications as part of the same project). Both aspects are set to be addressed before the submission of access requests becomes possible.

49 The portal can only be accessed with an EU login and the research institution can be selected from a list of all organisations that have applied for or received EU funding-based query to the Funding & Tenders Portal Organisation Public Data service API, which holds all organisations registered with a PIC and participating in EU programme, see European Commission (2025). EU Login - European Commission Authentication Service. https://wikis.ec.europa.eu/spaces/NAITDOC/pages/33529367/EU+Login+-+European+Commission+Authentication+Service, European Commission (2025). Funding & Tenders Portal Application Programming Interfaces (APIs). https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/support/apis

50 for example, through employment contracts, or other documentary proof of legal association.

51 for example, through their organisations statutes, or annual reports.

results publicly available without charge.[52] The application also needs to include details about the project's funding sources, including non-financial contributions.[53]

The description of the research itself takes up a less prominent role in the application. Specifically, the researchers only need to detail the research topic,[54] the systemic risk(s) studied,[55] and the planned research activities.[56] This is a noteworthy change from the draft delegated act (DDA) which included the requirement for researchers to include an abstract of their research project, which had raised concerns that such information allow platforms to tamper with the data to be accessed.[57] The final DA addresses this by reducing the information required about the project overall, with the portal additionally giving researchers more control about what information is shared with which party.[58]

The core of the data access application consists of descriptions of the requested data,[59] how they and the requested time frames for access are necessary and proportionate,[60] and the proposed access modalities.[61] With regard to the requested data, the fact that data catalogues might be incomplete, poses a significant challenge to researchers[62] – but should not deter them from requesting the data either way, even if they are not included in VLOPSE's public documentation.[63] The most demanding part however, will likely lie in determining the risk on the dimensions of confidentiality, data security and personal data protection related to

52 Art. 8(a) DA.

53 Art. 8(b) DA, the DSA data access portal requires information about the funding's nature (public or private) and country of establishment, the year in which it was obtained, and its duration.

54 Art. 8(g.i) DA, see also note 59.

55 While not specified in the DA, this follows directly from Art. 40(4) DSA.

56 Art. 8(f) DA.

57 Seiling, L., Ohme, J., Klinger, U. (2024), supra note 30.

58 Art. 8(g) DA also requires researchers to provide a summary of the application, including a description of the data requested as referred to in 8(c), the VLIOPSE from which data are requested, and the research topic. Notably, the portal includes two fields in which researchers can detail the research topic. One in the "research project-specific information" section and one in the section for the "summary of the application" Assuming that only the information in the latter section will be communicated to the platforms, researchers have the choice to disclose more information to the DSCs vetting their application. While it is to be expected that platforms will attempt to also gain access to more information about the reasoning behind the request, the responsibility lies on the DSCs to protect this important information asymmetry ensuring research integrity.

59 Art. 8(c), specified in terms of format, scope, attributes, as well as relevant metadata and documentation, and if possible, with reference with to the platforms' data catalogues.

60 Art. 8(d).

61 Art. 8(e).

62 see Goanta et al. (2025), supra note 32.

63 Neither DSA nor DA limit researcher requests to the data listed in the VLOPSE's data access catalogues. This means that even if the data is not listed in the catalogues, DSCs might still formulate a reasoned request based on the application. In this case, platforms can still claim to not have access to this data (see section "Amendment procedures for the reasoned request") but would need to propose "alternative means through which access may be provided to the requested data or other data" (Art. 40(6) DSA). Both the EC as well as platform researchers as a community are thus advised to vet the platforms' catalogues by comparing the data listed within them to data referenced in other documentation or employee presentations.

the requested access, as well as the subsequent determination and realisation of appropriate technical, legal and organisational measures to address them.[64]

Having compiled all relevant documentation, researchers can eventually submit the access application, initiating the first, timed step of the data access process.

Application vetting and initial formulation of the reasoned request

In most cases the DSC-E responsible for the formulation of the RR based on the submitted application will be the Coimisiún na Meán, the Irish DSC, given that most data providers have their EU establishment in Ireland. Thus, EU researchers are advised to initially send their applications to the DSC of the Member State of their research organisation (DSC-M)[65], allowing national DSCs to serve as a sort of buffer: based on harmonised vetting procedures[66], the application's completeness is evaluated first to check if the researcher has provided all necessary documents[67], which, if passed, is followed by an initial assessment during which data protection authorities and independent experts can be consulted. Eventually, the DSC-M either sends the initial assessment's results (consisting of an evaluation and an associated level of confidence) or a notice of a failed completeness check to the DSC-E. The DSC-E then either A) formulates a RR and publishes it on the DSA data access portal, or B) informs the principal researcher of the reasons why the RR could not be formulated. Either action must be taken after 80 working days,[68] which means that the DSCs have a total of four months to take the steps outlined above. Ideally, this is where the process ends for everyone involved and VLOPSEs provide the data access to the researchers, as specified in the RR.

64 Given that the data accessible through Art. 40(4) DSA may theoretically cover the full range of these different risk dimensions, many applications will likely reach at least moderate data protection risks and thus require an in-depth consideration of potential mitigation measures. While legal and organisational challenges can be addressed through well-documented data management capabilities and practices as well as sharing agreements, many institutions may lack the technical capacities for their technical realisation. Institutional cooperations are thus key to keep the data access provision in Art. 40(4) from becoming an exclusive privilege for the best-resourced research institutions. See also Art. 9(4) DA.

65 The DA introduces the term "Digital Services Coordinator of the research organisation" while the DSA Art. 40(9) states that "researchers may also submit their application to the Digital Services Coordinator of the Member State of the research organisation". Non-EU researchers can still send their applications to the DSC of establishment directly.

66 The development of which is currently coordinated by the French DSC, Arcom, as part of Working Group 3 of the European Board for Digital Services, as discussed in European Board for Digital Services (2025). Press statement of the European Board for Digital Services following its 14th meeting. https://digital-strategy.ec.europa.eu/en/news/press-statement-european-board-digital-services-following-its-14th-meeting

67 To this end the DA provides some helpful pointers, more closely specifying which documents can be considered during researcher vetting (e.g. employment contracts or any other form of legal association for affiliation; a declaration of independence of commercial interests relevant to the specific project; funding entity, amount, nature and duration; and commitment letters by the organisation and other documentation for the sake of meeting data protection, security and confidentiality requirements).

68 Art. 7(1) DA.

Amendment procedures for the reasoned request

According to Art. 40(5) DSA, platforms have the chance to hand in an amendment request within 15 days after receiving a reasoned request on two grounds: they do not have access to the data, or the provision of access poses significant risk to the security of their service or the protection of confidential information (i.e., trade secrets). The DSC-E must then inform the principal researcher that an amendment request is being processed[69] and evaluate whether the request is duly justified within 15 days.[70] In this time, the DSC-E may request both the platform and the principal researcher to provide additional information necessary for the assessment[71], at the end of which it can either reject the amendment request or produce an amended RR. If the DSC-E rejects the amendment request, the initially formulated RR stays valid.

Mediation procedures

Within 5 working days after receiving the decision on their amendment request, platforms can request a mediation.[72] If the DSC-E's decides to engage in mediation – given that its participation is voluntary[73] – it must assess whether the proposed mediator meets the required criteria[74] within the 20 working days it has to initiate the mediation.[75] In doing so, the DSC-E is also required to set a maximum duration for the mediations, which must not exceed 40 working days. During the mediation, the DSC-M and principal researcher may voluntarily join, if invited by the DSC-E.[76] In case mediation is successful, the RR is reformulated by the DSC-E. If the mediation fails[77], the most recent version of the RR remains valid.[78] In any case, VLOPSEs will have to bear the full cost of mediation.[79]

Table 1: The two modes of researcher data access according to the DSA and the DA.

	Art. 40(12) "public" data access	**Art. 40(4) "non-public" data access**
scope	if possible, real-time access to data, provided that it is publicly accessible in VLOPSEs' online interface by researchers	access to data

69 Art. 12(1) DA.

70 Art. 40(6) DSA.

71 Art. 12(4) DA.

72 Art. 13(1) DA.

73 Art. 13(2) and Rec. 22 DA.

74 Art. 13(5) DA.

75 Art. 13(4) DA.

76 Art. 13(7) DA.

77 which may be because no agreement is reached or the mediator ends the mediation, see Art. 13(10) DA.

78 Art. 13(12) DA.

79 Art. 13(6) DA.

	examples: *aggregated impression and engagement data of content from public pages/groups, or public figures, e.g. number of reactions, shares, or comments (Rec. 98 DSA)*	*examples:* *content prior to its removal by VLOPSEs (Rec. 97 DSA); profile information, relationship networks, individual-level content exposure and engagement histories, data related to content recommendations or ad targeting, results of A/B tests; data related to content moderation and governance, data related to goods or services provided or intermediated by the data provider (Rec. 13 DA)*
eligibility	researchers who meet the conditions set out in Article…	
		40(8a) DSA: affiliation to a research organisation[80]
	40(8b) DSA: independence from commercial interests	
	40(8c) DSA: disclosure of research funding	
	40(8d) DSA: capability to fulfil the specific data security and confidentiality requirements for the requested data, description of appropriate technical and organisational measures	
	40(8e) DSA: access to the data and the time frames requested are necessary for, and proportionate to, the research purposes (see purpose limitation)	
		40(8f) DSA: explicit purpose limitation
		40(8g) DSA: commitment to freely accessible publication of results, within a reasonable time period after completion
application procedure	application is directly submitted to and vetted by the VLOPSEs (see Fig. 1)	application is submitted to and vetted by the DSCs, which publish valid requests in the DSA data access portal and forward them to VLOPSEs (see Fig. 2)
purpose limitation	detection, identification and understanding of systemic risks in the Union, as set out pursuant to Art. 34(1)	a) detection, identification and understanding of systemic risks in the Union, as set out pursuant to Art. 34(1) b) assessment of the adequacy, efficiency and impacts of the risk mitigation measures, pursuant to Art. 35

80 as defined in Article 2, point (1) in European Parliament and Council of the European Union (2019) Directive 2019/790 on Copyright and Related Rights in the Digital Single Market, EP, CONSIL, 130 OJ L. http://data.europa.eu/eli/dir/2019/790/oj/eng

Simplified process for data access based on Art. 40(12) DSA

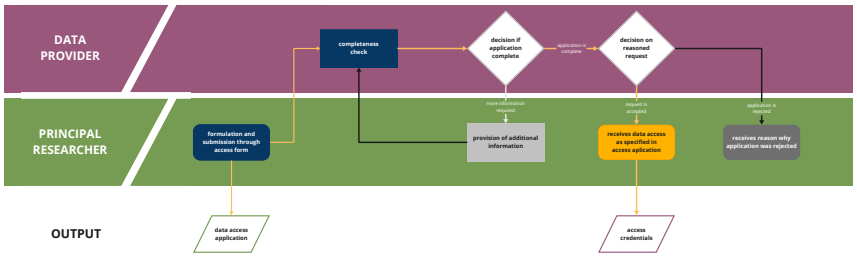
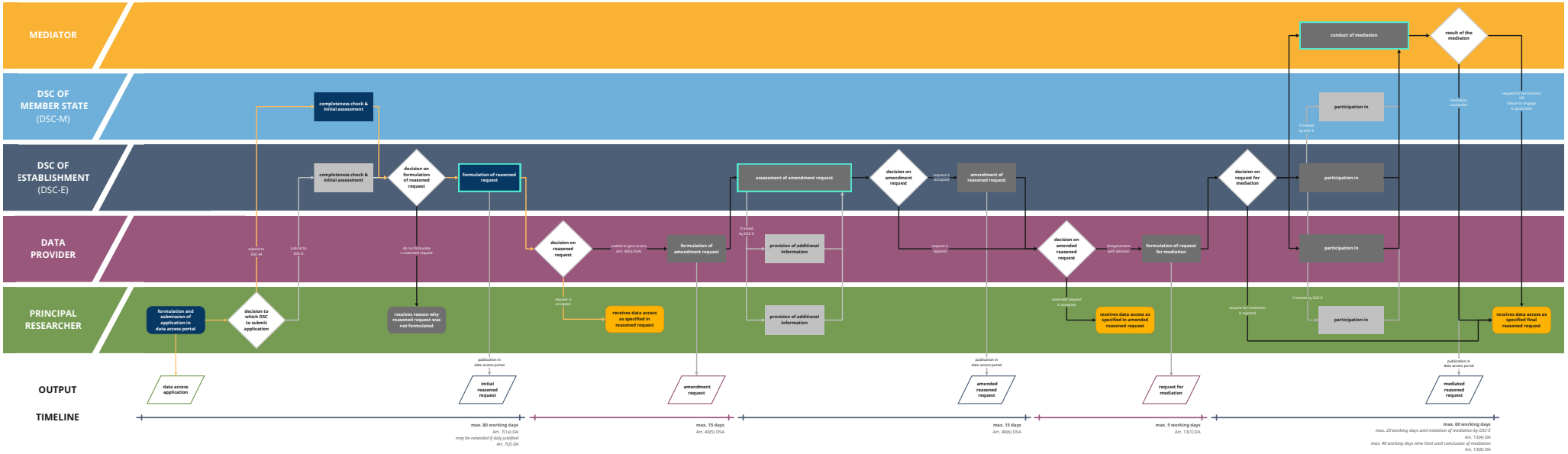


Figure 2: Process for data access under Art. 40(4) DSA as specified in the DA.

Simplified process for data access based on the delegated act on data access (DA) and Art. 40(4) DSA



4 Zooming Out: Realizing DSA Data Access in Fall 2025

Having reviewed the two kinds of data access in the DSA, it becomes clear that both come with existing and potential challenges in establishing an accessible and sustainable data access framework. How these challenges are addressed will largely influence the ultimate impact of the DSA's data access provision. Some of these issues are structural in nature; others may shift according to political winds. This last chapter of our Policy Paper has two goals: (1) accounting for dynamics beyond the legal text of the DSA and DA; and (2) contributing to a reflection on the necessary requirements for researcher data access, and by extension the DSA, to fulfil their potential.

Well-resourced, independent, and fair intermediaries

When considering conditions for functional implementation of the Art. 40 DSA's data access provisions, we can draw valuable lessons from another ambitious supranational European enforcement endeavour: the GDPR, which came into force in 2018 to establish a Data Protection Framework in the European territory. Like the DSA, the GDPR is based on the country-of-origin principle, meaning that the online activities it regulates are ultimately subject to the laws of the EU member state where the service provider is established. This creates a fragmented enforcement structure across the EU, requiring supervisory authorities to collaborate through harmonised procedures and standards. These conditions have arguably hindered effective GDPR enforcement, which also suffers from limited resources, weak coordination and inconsistent procedures amongst data protection agencies across EU member states—exacerbated by national political and bureaucratic differences. As a result of these compounding factors, data protection authorities continue to face significant obstacles in effectively processing complaints, conducting procedures and investigations, and sanctioning infringements.[81]

Considering that the DSA requires the DSCs to be completely independent[82] and to perform various tasks[83], including the 'impartial, transparent, and timely'[84] vetting of data access applications, it is clear that strong, efficient and fair authorities are key to a successful implementation of the DSA. While means for the harmonised processing of access applications are still in development,[85] national governments should avoid replicating known risks

81 European Union Agency for Fundamental rights (2024). GDPR in practice – Experiences of data protection authorities. https://fra.europa.eu/en/publication/2024/gdpr-experiences-data-protection-authorities

82 Art. 50(2) DSA.

83 Outside the data access context to VLOPSEs, DSCs are responsible for the supervision and enforcement of the DSA with regard to smaller intermediary services in their member state, as well as the certification of trusted flaggers and out-of-court dispute settlement bodies.

84 Art. 50(1) DSA.

85 supra note 66.

related to a lack of resources and coordination described above[86], by establishing supervisory authorities that are well-resourced, internationally coordinated and genuinely independent—yet still subject to public oversight. Currently, these requirements are only partially met throughout the EU member states.[87] If they are not properly accounted for and researchers from countries with less resourced or less independent DSCs may experience less support and longer waiting times, this would not only initially disadvantage those researchers. In the long term, it could also lead to the erosion or bypassing of national vetting mechanisms, as more researchers would directly apply to the Irish DSC for data access. Considering the DSA's implementation as an ambitious supranational endeavour, it is wise to invest in national enforcement authorities and their relationship to their peers.

Given the country-of-origin principle, data access intermediation is disproportionately centered in a single member state: Ireland. Indeed, as the section on privileged data access has shown, the Irish Coimisiún na Meán (CnaM) occupies a bottleneck position because it is the DSC of the EU member state where most VLOPSEs are established.[88] Accordingly, the requirements discussed above apply especially to the Coimisiún na Meán, which represents a single point of failure: it is the only DSC empowered to formulate and issue reasoned requests to the majority of platforms - and without any existing prioritisation mechanism could potentially be overburdened by too many requests made directly to the DSC. Researchers should thus be mindful of the intermediaries' capacity for vetting when selecting the time and recipient for sending their access request.

In this context, it is worth noting that there exists little prior experience with and little formal guidance for research data access procedures like the ones set out in the DSA. Thus, initial vetting will likely be slow and strict, possibly resulting in few accepted applications, as DSCs set towards building a solid foundation and replicable example with the first successful requests. It is important for both DSCs and researchers to understand this process as a

86 Which are not limited to the GDPR but also affect other policy areas like consumer or environmental protection, see for example Cantero Gamito, M., & Micklitz, H.-W. (2023) Too much too little? Assessing the Consumer Protection Cooperation (CPC) Network in the protection of consumers and children on TikTok. BEUC. https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-018_Assessing_CPC_Network_in_the_protection_of_consumers_and_children_on_TikTok-Report.pdf or Krämer, L. (2018). Dieselgate and the Protection of the Environment by Public Authorities. In E. Maitre-Ekern, E., Dalhammar, C. & Bugge, H. C. (Eds.), Preventing Environmental Damage from Products: An Analysis of the Policy and Regulatory Framework in Europe (pp. 153–175), Cambridge: Cambridge University Press.

87 for an analysis of the national DSCs in Bulgaria, Croatia, Czech Republic, Germany, Italy and Romania on the dimensions legal independence, political interference and leadership selection, private sector influence, as well as accountability and transparency, see Civil Liberties Union for Europe. (2025). Monitoring the implementation of the Digital Services Act: The independence of Digital Services Coordinators. https://dq4n3btxmr8c9.cloudfront.net/files/0ol1bo/Liberties_DSA_Monitoring_Febr2025.pdf; for information on the staffing of the German DSC (having staffed 48 of the 70,6 positions required by the German implementation of the DSA), see Windwehr, S. (2024). Geschichten aus dem DSC-Beirat: Was ist eigentlich dieser Digital Services Act?. Netzpolitik.org. https://netzpolitik.org/2024/geschichten-aus-dem-dsc-beirat-was-ist-eigentlich-dieser-digital-services-act/

88 As such, CnaM has been actively preparing for what, according to a survey among researchers, will likely be around 450 applications in the first six months. For more preliminary information of the survey results see Coimisiún na Meán (2025). An Coimisiún: Vetted Researcher Newsletter Issue 1. https://mailchi.mp/cnam.ie/vetted-researcher-newsletter-issue-1 or Institute for Information Law (2025). Researcher Access in the DSA State of Play and Next Steps. CPDP.ai 2025. https://youtu.be/Qu6SMafb-hM?t=2075

collaborative exercise, not unlike an experiment in which knowledge (in this case shared standards for access applications) emerges from trial and error. While such a high chance of initial failure is sure to frustrate many researchers, constructive engagement with the DSCs is a key foundational condition for both the start and the future of data access.

Platform cooperation

By adopting an institutional arrangement close to enforced self-regulation,[89] the DSA largely relies on the consent and cooperation of regulated entities to deliver results. Thus, as much as it stipulates means of coercion and applicable sanctions[90], it still operates within the logics of engaging—and some might even argue, privileging[91]—corporate power in the regulatory process. While this is true for the DSA's risk management provisions generally,[92] it particularly applies to the fundamentals of data access: its value for knowledge creation depends largely on platforms, as they determine what data to make available and under what conditions.

Although the process for privileged data access, as outlined above, foresees that such decisions will soon be made by the DSCs based on researchers' access applications, platforms remain in a structurally dominant position, as the implementation of request-specific access modalities will rest upon their compliance with the DSCs' requests. Yet, meaningful data access—essential for understanding risks in dynamic digital environments—requires platforms to move beyond passive, compliance-driven interactions with researchers. Instead, what is needed is active outreach, transparent participation mechanisms and genuine readiness to collaboratively work towards the conditions that allow for accessible and flexible data access by researchers. And although platforms have already proactively engaged researchers on occasion[93], more structural means of engagement are yet to fully materialise. Thus, platform compliance is the baseline, but platform cooperation the goal—with both resting on a presumption of good faith[94] and aligned policy goals.[95]

Unfortunately, there are reasonable grounds to question these presumptions. The EC has already acknowledged that platforms face considerable compliance costs when implementing the DSA (which would only grow in case of full platform cooperation) as well as additional

89 Von Bernuth, N. (2025). The Premise of Good Faith in Platform Regulation. https://doi.org/10.59704/5494324c1cc2203d

90 see Art. 52 DSA.

91 Griffin, R. (2025). Governing platforms through corporate risk management: The politics of systemic risk in the Digital Services Act. European Law Open, 1–31. https://doi.org/10.1017/elo.2025.17

92 As an example of management-based regulation), the DSA shifts the responsibility on the appropriate path of risk management to the actor with the most information, effectively relying on platforms' self-assessment.

93 supra note 42.

94 Von Bernuth, N. (2025)., supra note 89.

95 Harfst, J.-O. (2025). Wahlen in der wehrhaften Plattform-Demokratie. Verfassungsblog. https://doi.org/10.59704/2b1064b931db2128

costs following potential enforcement action by the authorities.[96] It is reasonable to assume that VLOPSEs as private actors are less interested in the completion of the DSA's policy goals than they are in cost-efficient compliance that does not threaten their dominant market position. The resulting response to regulation is one of minimal compliance, indications to which can be observed at various points of the DSA's implementation[97], shining a spotlight onto potential shortcomings in its enforcement structure.

Considering that most VLOPSEs are American or Chinese companies, their willingness to effectively cooperate and comply with the DSA should also be considered against a geoeconomic backdrop, in which economic instruments are used to further national interests and geopolitical goals.[98] Both Chinese and US platform companies have been described as deeply entangled with the state[99] and while previous attempts of US governments to influence the regulation of US tech platforms elsewhere have arguably been more subtle[100], the second Trump administration has demonstrated their willingness to disrupt geopolitical relationships in favour of American platform companies' commercial interests.[101]

---

96 European Commission. 2020. IMPACT ASSESSMENT Accompanying the Document PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a Single Market For Digital Services (Digital Services Act) and Amending Directive 2000/31/EC. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52020SC0348

97 In the context of data access, see the discussion on issues with access to publicly available data above or Jaursch, J., Ohme, J., & Klinger, U. (2024). Enabling Research with Publicly Accessible Platform Data: Early DSA Compliance Issues and Suggestions for Improvement. Weizenbaum Policy Paper, 9. http://www.doi.org/10.34669/WI.WPP/9; in the context of the first round of risk and audit reports published at the end of 2024, see Holznagel, D. (2025). Shortcomings of the first DSA Audits — and how to do better. DSA Observatory. https://dsa-observatory.eu/2025/06/11/shortcomings-of-the-first-dsa-audits-and-how-to-do-better

98 Blackwill, R. D., & Harris, J. M. (2016). What Is Geoeconomics? In R. D. Blackwill & J. M. Harris, War by Other Means: Geoeconomics and Statecraft. The Belknap Press of Harvard University Press., see also Babić, M., Dixon, A. D., & Liu, I. T. (Eds). (2022). The Political Economy of Geoeconomics: Europe in a Changing World. Springer International Publishing. https://doi.org/10.1007/978-3-031-01968-5

99 Rolf, S., & Schindler, S. (2023). The US–China rivalry and the emergence of state platform capitalism. Environment and Planning A: Economy and Space, 55(5), 1255–1280. https://doi.org/10.1177/0308518X221146545

100 Akhtar, S. I., & Sutherland, M. D. (2021). Digital Trade and U.S. Trade Policy. Congressional Research Service. https://www.congress.gov/crs-product/R44565, Mirrlees, T. (2020). Weaponizing the Internet and World Wide Web for Empire: Platforming Capitalism, Data-Veillance, Public Diplomacy, and Cyberwarfare. In O. Boyd-Barrett & T. Mirrlees (Eds), Media Imperialism: Continuity and Change. Rowman & Littlefield.

101 It is worth noting that before the US administration started to hold hearings about "Europe's Threat to American Speech and Innovation", and tariffs on countries regulating American tech companies more generally, it engaged in similar pressure tactics towards Brazil: the second named reason provided by Donald Trump for a 50 % import tariff on Brazilian goods in July 2025 referenced the Brazilian Supreme Court Decision ruling that social media platforms were liable for their users' posts. Shortly after, the Office of the United States Trade Representative issued a vague statement expressing concerns that "Brazil may harm the competitiveness of American companies operating in digital commerce and electronic payment services", which was interpreted as a response to the release of a payment service developed by the Brazilian central bank which would compete with Meta's planned rollout of WhatsApp payments as well as American credit and debit card companies. See Boak, J. (2025, July 30). Trump signs order to justify 50% tariffs on Brazil. AP News. https://apnews.com/article/trump-brazil-tariffs-bolsonaro-lula-trade-imbalance-de4cf0669b00a76149e8f39f200af502, House Judiciary Committee Republicans. (2025, September 3). Europe's Threat to American Speech and Innovation. http://judiciary.house.gov/committee-activity/hearings/europes-threat-american-speech-and-innovation, Moreira, P. T. (2025, July 17). Analysis: How Pix stepped on Zuckerberg's toes. Valor International. https://valorinternational.globo.com/markets/news/2025/07/17/analysis-how-pix-stepped-on-zuckerbergs-toes.ghtml, Sasipornkarn, E., & Camino Gonzalez, J. (2025, June 12). Brazil rules social media platforms liable for users' posts. Deutsche Welle.

In the transatlantic context, US actors have repeatedly denounced the DSA as protectionist or censorious.[102] While these allegations might seem contradictory when contrasting current free speech practices in the US context[103] to European platform regulation, which does not entail any obvious censorship threats,[104] they add further charge to an already tense relationship. At present, despite the confrontational rhetoric of the US administration and questionable actions taken by platforms,[105] US tech companies still derive a substantial share of their global revenue from the EU,[106] likely making market access too valuable to jeopardise for political posturing. This economic interdependence will presumably limit the scope of US pushback and incentivise at least nominal compliance with EU regulation. Still, it will likely not guarantee the necessary cooperation described above, which means that researcher-

https://www.dw.com/en/brazil-rules-social-media-platforms-liable-for-users-posts/a-72877466, Sweney, M. (2025, August 26). Trump threatens tariffs on countries that 'discriminate' against US tech. The Guardian. https://www.theguardian.com/us-news/2025/aug/26/donald-trump-tariffs-us-tech-uk-digital-services-tax-eu

102 Iglesias Keller, C., Ohme, J., Seiling, L., Neuberger, C. (2025): Regulating Digital Platforms in Times of Democratic Crisis – What is Next for Germany and the EU? (Weizenbaum Discussion Paper; 45). Weizenbaum Institute. https://doi.org/10.34669/wi.dp/45, House Judiciary Committee Republicans. (2025, July 25). The Foreign Censorship Threat: How the European Union's Digital Services Act Compels Global Censorship and Infringes on American Free Speech. http://judiciary.house.gov/media/press-releases/foreign-censorship-threat-how-european-unions-digital-services-act-compels, Rubio, M. (2025, May 28). Announcement of a Visa Restriction Policy Targeting Foreign Nationals Who Censor Americans. United States Department of State. https://www.state.gov/announcement-of-a-visa-restriction-policy-targeting-foreign-nationals-who-censor-americans/

103 Hickey, D., Fessler, D. M. T., Lerman, K., & Burghardt, K. (2025). X under Musk's leadership: Substantial hate and no reduction in inauthentic activity. PLOS ONE, 20(2), e0313293. https://doi.org/10.1371/journal.pone.0313293, Day, M., & Ford, B. (2025, August 26). Microsoft Asked FBI for Help Tracking Palestinian Protests. Bloomberg Law. https://news.bloomberglaw.com/tech-and-telecom-law/microsoft-asked-fbi-for-help-tracking-palestinian-protests, Farah, H. (2023, October 26). Pro-Palestinian Instagram account locked by Meta for 'security reasons'. The Guardian. https://www.theguardian.com/technology/2023/oct/26/pro-palestinian-instagram-account-locked-by-meta-for-security-reasons, Fischer, S. (2025, January 16). Google won't add fact-checks despite new EU law. Axios. https://www.axios.com/2025/01/16/google-fact-check-eu, Gkritsi, E. (2025, May 8). Musk's X blocks account of jailed Erdoğan rival. POLITICO. https://www.politico.eu/article/x-blocks-account-of-turkish-opposition-leader/, McMahon, L., & Tidy, J. (2023, October 20). Instagram sorry for adding 'terrorist' to some Palestinian user bios. BBC. https://www.bbc.com/news/technology-67169228

104 Keller, D. (2025, September 2). A Primer on Cross-Border Speech Regulation and the EU's Digital Services Act. Stanford CIS. https://cyberlaw.stanford.edu/blog/2025/09/a-primer-on-cross-border-speech-regulation-and-the-eus-digital-services-act/

105 Evidence in the recently released report by the U.S. House of Representatives Judiciary Committee (supra note 102) included "confidential information from EU workshops, emails between the EU executive and companies, content takedown requests in France, Germany and Poland and readouts from Commission meetings with tech firms" likely provided by participating platforms, see Gkritsi, E. (2025, July 25). US Congress goes after EU over 'foreign censorship'. POLITICO. https://www.politico.eu/article/us-congress-eu-digital-services-act-foreign-censorship/

106 For example, in their SEC filings for 2024 Meta reported ~ 23 % of their revenue was generated in Europe, Apple reported ~ 26 % of net sales to be coming from Europe, while Amazon reported that ~ 6 % of net sales occurred in Germany alone. Other VLOPSEs do not provide data on a similar level of disaggregation, see Amazon.com, Inc. (2025). ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934. https://www.sec.gov/ix?doc=/Archives/edgar/data/0001018724/000101872425000004/amzn-20241231.htm, Apple Inc. (2024). ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934. https://www.sec.gov/ix?doc=/Archives/edgar/data/0000320193/000032019324000123/aapl-20240928.htm, Meta Platforms, Inc. (2025). ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934 (Nos 001–35551). https://www.sec.gov/ix?doc=/Archives/edgar/data/0001326801/000132680125000017/meta-20241231.htm

platform relationships will continue to be open for dispute that may involve interests beyond access to data.

Robust public enforcement & fostering of institutional innovation

According to Art. 56(2) DSA, the European Commission (EC) exclusively supervises and enforces all risk-related DSA provisions, including data access. At the time of writing, DG CNECT, the responsible Directorate-General inside the EC, has opened 14 proceedings, 7 of which explicitly refer to researcher data access.[107] The fact that the first of these proceedings has been settled by AliExpress through binding commitments to broad data access measures[108] may cautiously be taken as an encouraging precedent for the future of DSA-based data access, particularly considering DG Connect's lack of prior enforcement experience.[109]

Nevertheless, decisions on US platforms remain pending. Proceedings against X, in particular, have been repeatedly linked to transatlantic trade and security negotiations, raising concerns that the EC may be tempering its DSA enforcement.[110] This is where the EC's role as both a political actor and an enforcement body creates complications, as it risks enforcement being used as a bargaining chip in political negotiations. However, although recent actions seem to indicate the contrary,[111] the EC has denied these claims, framing enforcement of EU regulation as non-negotiable.[112] While it may appear self-evident that regulation must be enforced, the EC should maintain this firm stance to ensure that the basic conditions for data

107 see European Commission. (2025). Supervision of the designated very large online platforms and search engines under DSA. https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses, esp. regarding the proceedings against AliExpress (started on 14.03.2024), TikTok (started on 17.12.2024), Facebook and Instagram (started on 30.04.2024), TikTok (started on 19.02.2024), X (started on 18.12.2023), and Temu (started on 31.10.2024).

108 namely a dedicated research API, scraping, and dedicated datasets. See European Commission. (2025). Commission makes AliExpress' commitments under the Digital Services Act binding. https://digital-strategy.ec.europa.eu/en/news/commission-makes-aliexpress-commitments-under-digital-services-act-binding

109 Vergnolle, S. (2023). A New European Enforcer? Verfassungsblog. https://doi.org/10.17176/20230523-140352-0

110 Bade, G., & Mackrael, K. (2025, June 21). U.S., EU Near Deal on Nontariff Trade Irritants. The Wall Street Journal. https://www.wsj.com/economy/trade/u-s-eu-near-deal-on-non-tariff-trade-irritants-455c42f1, Gustaf Kilander. (2024, September 17). JD Vance says US could veto NATO if Europe tries to regulate Elon Musk's platforms. The Independent. https://www.independent.co.uk/news/world/americas/us-politics/jd-vance-elon-musk-x-twitter-donald-trump-b2614525.html, Hickey, D., Fessler, D. M. T., Lerman, K., & Burghardt, K. (2025). X under Musk's leadership: Substantial hate and no reduction in inauthentic activity. PLOS ONE, 20(2), e0313293. https://doi.org/10.1371/journal.pone.0313293, Satariano, A. (2025, April 3). E.U. Prepares Major Penalties Against Elon Musk's X. The New York Times. https://www.nytimes.com/2025/04/03/technology/eu-penalties-x-elon-musk.html

111 Crofts, L., Vasant, K., & Hirst, N. (2025, September 1). Google's adtech fine pulled at last minute over EU-US trade tensions. MLex. https://www.mlex.com/mlex/articles/2382762/google-s-adtech-fine-pulled-at-last-minute-over-eu-us-trade-tensions, Foy, H., & Moens, B. (2025, July 17). Brussels stalls probe into Elon Musk's X amid US trade talks. Financial Times. https://www.ft.com/content/8f38514b-3265-496e-91e2-f8a44daa0ab6

112 Chee, F. Y., Blenkinsop, P., & Chee, F. Y. (2025, June 30). EU trade chief bound for US, seeking deal fair for both sides. Reuters. https://www.reuters.com/sustainability/boards-policy-regulation/eu-tech-rules-not-included-us-trade-talks-eu-commission-says-2025-06-30/, Datta, A. (2025, September 1). Virkkunen defends 'sovereign' DSA, DMA against MAGA attacks. Euractiv. https://www.euractiv.com/section/tech/news/virkkunen-defends-sovereign-dsa-dma-against-maga-attacks/

access are provided.[113] After all, the EC has a self-interest in a working data access regime, as it will be able to draw on the findings for future regulatory action[114] and is bound by the Charter of fundamental rights of the European Union which includes a commitment to academic freedom.[115]

As discussed in the section on access to publicly available data, effective data access for researchers is currently obstructed by opaque vetting procedures, data quality issues and the lack of legal clarity regarding scraping. While the EC could provide additional guidance through another delegated act[116], it is more likely to promote soft law instruments such as voluntary standards[117] and codes of conduct[118] to address these issues. In this context, the EC could build on emerging institutional innovation[119], as researchers begin to organise procedures and develop tools and best practices to streamline both the application process as well as data access itself.

The EC can help foster and formalise such initiatives—working in tandem with VLOPSEs—through the soft law instruments mentioned above, provided platforms are willing to collaborate. Putting these concepts into practice could prove an important path towards both addressing the inherent imbalance of power in favour of data providers in platform data access, and even in setting the narrative on systemic risk. The Code of Conduct on Disinformation shows that this approach to governance can produce results even though it also exposes its limitations: it rises and falls with platform cooperation[120], and even if platforms engage constructively, such developments require significant upfront effort and resource investment from researchers—and, crucially, take time during which existing power imbalances remain

113 Ohme, J., Seiling, L, de Vreese, C. (2025). Will Europe Sacrifice the Digital Services Act in Negotiations with Trump?. Tech Policy Press. https://www.techpolicy.press/will-europe-sacrifice-the-digital-services-act-in-negotiations-with-trump/

114 Leerssen, P. (2024). Outside the Black Box: From Algorithmic Transparency to Platform Observability in the Digital Services Act. Weizenbaum Journal of the Digital Society, 4(2). https://doi.org/10.34669/WI.WJDS/4.2.3

115 Art. 23 CFR.

116 the passing of which would likely again take years.

117 Art. 44 DSA.

118 Art. 45 DSA, Rec. 103 DSA.

119 see Fertmann, M., Ganesh, B., Gorwa, R., & Neudert, L.-M. (2022). Hybrid institutions for disinformation governance: Between imaginative and imaginary. Internet Policy Review. https://policyreview.info/articles/news/hybrid-institutions-disinformation-governance-between-imaginative-and-imaginary/1669, or AlMalki, H. A., & Durugbo, C. M. (2023). Systematic review of institutional innovation literature: Towards a multi-level management model. Management Review Quarterly, 73(2), 731–785. https://doi.org/10.1007/s11301-022-00259-8 for a more general overview of institutional innovation in the sense of internal processes.

120 Meta just recently refused to sign Brussel's Code of Practice on General Purpose AI and many platforms withdrew from key commitments in the Code of Conduct on Disinformation when it was integrated into the DSA framework from a Code of Practice, see Gkritsi, E., & Haeck, P. (2025, July 18). Meta rebuffs Brussels over AI rules. POLITICO. https://www.politico.eu/article/meta-wont-sign-eu-ai-code/, Alvarado Rincón, D., & Meyer-Resende, M. (2025). Big tech is backing out of commitments countering disinformation—What's Next for the EU's Code of Practice?. Democracy Reporting International. http://democracy-reporting.org/en/office/EU/publications/big-tech-is-backing-out-of-commitments-countering-disinformation-whats-next-for-the-eus-code-of-practice

unaddressed. This will likely lead to disputes which need settlement, in the form of independent experts, as suggested by the DSA and outlined by the EDMO working group.[121]

Researcher organisation

Building an accessible and sustainable data access framework requires the collaboration of actors with divergent motivations. Having already discussed to what extent the platforms' and the EC's goals align with this agenda, researchers need to consider how they position themselves vis-a-vis the other actors. After all, they have to navigate the challenges to academic freedom that come with the purpose limitations associated with the DSA's data access regime[122], the fact that their findings will likely be used for further regulatory action and the unequal distribution of responsibilities in the current configuration of the data access system.

Indeed, as the EC only seems to have limited capacity to engage in self-organised user and evidence gathering, it is mostly on researchers to point towards shortcomings of the current setup, like problems during the application process or data quality issues. While this information has the potential to steer and inform ongoing proceedings by the EC, they do not directly address the highlighted issues—which in turn means that researchers need to withdraw resources from their actual research to fill in the gaps left by the legislator.[123]

Strategic boundary work

As it stands, even after the publication of the DA, many open questions regarding the specific implementation of data access remain. Researchers, however, are in a position not merely to operate within the DSA's data access framework, but to actively and strategically shape and clarify its contours by engaging in a form of boundary work: the construction, negotiation, enactment and contestation of boundaries.[124]

One area requiring such boundary work concerns the existing and potential range of data types and access modalities available. Most platforms currently interpret 'publicly accessible data' narrowly (typically limited to content metadata), thereby excluding other publicly available elements such as the content itself, user interface design or potential aggregate data

121 European Digital Media Observatory. (2024). Report on the EDMO DSA Data Access Pilot. European Digital Media Observatory. https://edmo.eu/wp-content/uploads/2024/12/Report-on-the-EDMO-DSA-Data-Access-Pilot.pdf

122 Mast, T. (2024). Forschungsdatenzugang und Technologieregulierung. Wissenschaftsrecht, 57(2), 101. https://doi.org/10.1628/wissr-2024-0011

123 The DSA40 Data Access Collaboratory's Issue Tracker (https://dsa40collaboratory.eu/issue-tracker/) attempts to collect and highlight issues encountered by researchers in order to make other researchers, regulators and platforms aware of existing barriers to research access.

124 originally Gieryn, T. F. (1983). Boundary-Work and the Demarcation of Science from Non-Science: Strains and Interests in Professional Ideologies of Scientists. American Sociological Review, 48(6), 781-795. https://doi.org/10.2307/2095325; see also Lamont, M., & Molnár, V. (2002). The Study of Boundaries in the Social Sciences. Annual Review of Sociology, 28(1), 167-195. https://doi.org_/doi/10.1146/annurev.soc.28.110601.141107

provided as dedicated datasets (e.g., highly disseminated content).[125] Similarly, while the draft DA mentioned various examples for data types and data transfer as well as secure processing environments (SPEs) as potential access modalities, in their responses many researchers pushed for these examples to be extended.[126] However, no additional examples were included in the final DA, which means that the actual extent of the DSA's access framework remains unclear.[127] While the data access process provides a rough and potentially lengthy roadmap for how more potential data types and access modalities could be uncovered, attempting to clarify these gaps still requires the researchers to invest time and resources into access applications with an uncertain outcome—making "boundary labour" a more fitting term in this context.

Even though data access applications can help clarify the availability of certain data types and modalities, they cannot resolve broader legal ambiguities in the DSA's access provisions. In this context, private enforcement[128], or strategic litigation in particular, can be not only a tool to deal with straightforward non-compliance but also a mechanism for addressing non-compliance, as well as clarifying, securing, or affirming legal interpretations that will effectively operationalise Article 40 of the DSA. This has recently been demonstrated by a lawsuit the CSO Democracy Reporting International brought against X: Although the court denied the specific request, it clarified that Art. 40 (12) is to be interpreted as conferring a subjective right[129] from which it also concluded that the matter can be litigated in the EU country where the research project is taking place.[130] While these clarifications constitute a significant precedent for enforcement of the DSA's provisions, strategic litigation requires resources as well as institutional support, which might be more easily organised by researchers working for CSOs than for academic institutions, which tend to be more risk-averse.

Another particularly consequential site for boundary work is the scope of systemic risk within the DSA framework. As Griffin argues, the DSA risks boundary reinforcement if corporate risk management is privileged over public interest research.[131] Researchers, therefore, play a vital role in contesting overly narrow definitions by identifying and documenting under-recognised risks, investigating broader sociopolitical harms and countering the DSA's

125 as suggested by Rec. 98 DSA and the commitments made by AliExpress, see supra note 108.

126 Seiling, L., Ohme, J., Klinger, U. (2024), supra note 30.

127 For example, the possibilities of receiving internal data (not bound to or created by the users on the platform but to the VLOPSEs as organisations) or data inferred by the platforms, as well as testing the platforms' systems through modalities, such as researcher sandboxes, as of yet remain speculative and open to interpretation.

128 Leerssen, P., van Duin, A., Toepoel, I., & van Hoboken, J. (2025). Pathways to Private Enforcement of the Digital Services Act (DSA). DSA Observatory. https://dsa-observatory.eu/wp-content/uploads/2025/06/DSA-Private-Enforcement-final-draft.pdf

129 holding that Article 40(12) DSA imposes both positive and negative obligations, to generally provide and to not restrict access respectively.

130 Democracy Reporting International (2025) DSA in Court: What we learned from suing X. Democracy Reporting International. https://democracy-reporting.org/en/office/global/news/dsa-in-court-what-we-learned-from-suing-x; the report also includes a helpful list of tips for researchers, encouraging them to 1) act quickly, 2) consult legal teams early, 3) clarify financial and institutional support; and 4) prepare a strong application.

131 Griffin, R. (2025). Governing platforms through corporate risk management: The politics of systemic risk in the Digital Services Act. European Law Open, 1–31. https://doi.org/10.1017/elo.2025.17

rather technocratic approach through participatory science, co-creating knowledge in tandem with underrepresented populations and affected groups.[132]

Resilient independent infrastructure

Research data access comes with a set of technical challenges, especially when the access modalities involve data transfer or other means of data access set up independently of platforms' infrastructures. In these cases, researchers are required to provide adequate data privacy and security safeguards[133], which, if the requested data is especially sensitive, may require access to significant expertise and resources that only a minority of researchers and research institutions can draw on. Even if researchers follow ethical data handling practices, those without institutional support are structurally disadvantaged in accessing and working with such data.

To address this imbalance and to allow for more research on systemic risk, independent infrastructures which can facilitate the storage and processing of large-scale high sensitivity data are needed. Building such infrastructure from scratch would be both time- and resource-intensive. Moreover, doing so would also overlook established institutions: the life sciences have long stored, transferred and processed sensitive genetic data and developed mature infrastructure[134] to allow for such processing. Collaborating with these established institutions, or scaling their existing solutions, offers a more efficient and inclusive path forward. Archiving institutions[135] could also play an important role in researcher data access by storing data accessed through data transfer mechanisms. With appropriate vetting procedures in place to ensure that only eligible researchers gain access, their archives could facilitate easy replication of research and would eliminate the necessity for redundant access requests. If they meet the criteria for Secure Processing Environments[136], they would offer another crucial access pathway for researchers without adequate institutional infrastructure.

Technical infrastructure is also needed to ensure data quality checks. Notably, Recital 13 of the DA introduces "evidence of poor quality or unreliability of such data deriving from other sources" as a potential justification for an access application. In this context, "other sources" likely refer to data access modalities accessible for researchers under Art. 40(12) DSA, which have been repeatedly criticised for data quality issues regarding completeness or accuracy.[137] With regards to other platform data, some researchers have even raised concerns about

---

132 positive examples include the Data Workers Inquiry that pioneers research on equal grounds with a group key to online safety but missing from the DSA: content moderators, see https://data-workers.org/, and relatedly Miceli, M., Tubaro, P., Casilli, A. A., Le Bonniec, T., Wagner, C. S., & Sachenbacher, L. (2024). Who Trains the Data for European Artificial Intelligence? https://hal.science/hal-04662589/document

133 Art. 40(8d) DSA applies to both modes of research data access specified in Art. 40.

134 see, for example, https://elixir-europe.org/

135 for an overview of the European, Swiss, and UK data archives see UK Data Service (2025). European data archives. https://ukdataservice.ac.uk/help/other-data-providers/data-archives/european-data-archives/, see also supra note 21.

136 supra note 40.

137 supra note 26.

willful tampering.[138] Thus, while the DA seems to recognise these concerns, it does not put in place any provisions to ensure the quality of the data received through its access process. If the EC does not assume responsibility to ensure that VLOPSEs provide high-quality data, researchers are left with two poor options: either accept unverified data or invest significant resources in validating it themselves.[139] Neither outcome is ideal, as both risk compromising the quality of the knowledge produced as well as the effective mitigation of systemic risks. One potential solution is for researchers to collaboratively establish validation services, possibly hosted and developed in collaboration with the same infrastructures mentioned earlier, that researchers could consult to easily review the accessed data before using it in research projects.

Both infrastructures described are key for maintaining researcher independence and ensuring platform accountability. To be truly effective, these systems should be resilient, meaning they have the 'ability to prepare and plan for, absorb, recover from, and more successfully adapt to adverse events'.[140] In practice, this means, among other this, decentralisation, redundancy, and modularity[141] so that no single failure—be it closure, litigation or withdrawal for other reasons—can undermine the service provision, incentivising meaningful collaboration, division and labour, and planning between institutions from various member states. In parallel, researchers without strong institutional ties could explore smaller-scale, low-cost solutions for the provision of resilient services.[142]

Coordination and intermediation

As the above sections have shown, researchers play a key role in shaping the development of the DSA-based data access framework to ensure that it lives up to its potential and meets their needs. However, addressing these challenges requires more time and resources than individual researchers can reasonably provide. Thus, the way forward lies in researchers organizing collectively—through coordination and intermediation—to pool resources, share information and jointly develop procedures, tools and best practices to work together towards the shared goal of accessible and sustainable research data access.

---

138 Bagchi, C., Menczer, F., Lundquist, J., Tarafdar, M., Paik, A., & Grabowicz, P. A. (2024). Social media algorithms can curb misinformation, but do they?. Science eLetter. https://www.science.org/doi/10.1126/science.abp9364#eletterModalToggler also available at https://arxiv.org/abs/2409.18393

139 see the discussion of scraping as an access modality in the section "How does it work for publicly accessible data?"

140 National Research Council. (2012). Disaster Resilience: A National Imperative (p. 13457). National Academies Press. https://doi.org/10.17226/13457, p. 1.

141 Gilrein, E. J., Carvalhaes, T. M., Markolf, S. A., Chester, M. V., Allenby, B. R., & Garcia, M. (2021). Concepts and practices for transforming infrastructure from rigid to adaptable. Sustainable and Resilient Infrastructure, 6(3–4), 213–234. https://doi.org/10.1080/23789689.2019.1599608

142 Sathiaseelan, A., Selimi, M., Molina, C., Lertsinsrubtavee, A., Navarro, L., Freitag, F., Ramos, F., & Baig, R. (2017). Towards decentralised resilient community clouds. Proceedings of the 2nd Workshop on Middleware for Edge Clouds & Cloudlets - MECC '17, 1–6. https://doi.org/10.1145/3152360.3152363, Von Tottleben, A., Ihle, C., Schubotz, M., & Gipp, B. (2021). Academic Storage Cluster. 2021 ACM/IEEE Joint Conference on Digital Libraries (JCDL), 278–279. https://doi.org/10.1109/JCDL52503.2021.00034.

Coordination to reach a common goal spans a range of activities, such as action alignment and information sharing among a group of actors, and can result in more efficient use of resources, increased strategic capacity to address complex problems, enhanced learning and a higher quality of outcomes generally.[143] A notable example of coordination in the DSA's broader risk governance framework is the initial analysis of VLOPSEs' risk assessment reports by 40 different CSOs, organised as the DSA Civil Society Coordination Group.[144] Similar coordination occurred during the feedback period on the draft delegated act on data access[145] and in the legal case of DRI against X.[146] Legal support, in particular, is an area where researchers would benefit from deeper coordination, especially in preparing for the potential of becoming targets of litigation themselves.[147] Shared data access requests can also enhance the success of boundary work on data accessibility, particularly when targeting publicly available data and bypassing the lengthier processes outlined in the DA. Coordination in open-source software development could further streamline the processing of accessed data: implementation of tools like API wrappers or graphical user interfaces (GUIs) that enable low- or no-code access could lower barriers for researchers. In addition, the joint development of data dictionaries and ontologies could support cross-platform research.

Intermediation refers to processes or organisations that link or broker between different actors for purposes of information or knowledge scanning and processing, or the development, testing, validation and provision of technologies and standards.[148] Here too, notable

143 Provan, K. G., & Kenis, P. (2007). Modes of Network Governance: Structure, Management, and Effectiveness. Journal of Public Administration Research and Theory, vol. 18, no. 2, pp. 229–252. https://doi.org/10.1093/jopart/mum015

144 DSA Civil Society Coordination Group. (2025). Initial Analysis on the First Round of Risk Assessments Reports under the EU Digital Services Act. https://cdt.org/wp-content/uploads/2025/03/RA-Report-Assessment-Report.pdf

145 In November 2024, the Coalition of Independent Technology Research hosted information sessions on the Delegated Act, opening the space for a community discussion around potentials and limits of potential feedback as well as identifying key areas of concern for researchers.

146 CITR. (2025, May 15). A Win for Democracy, Transparency, and Research: Standing alongside DRI and GFF. Coalition for Independent Technology Research. https://independenttechresearch.org/a-win-for-democracy-transparency-and-research-standing-alongside-dri-and-gff/

147 In this context, experiences of American researchers experiencing legal pressure by politicians and platform owners – as in the cases of the Stanford Internet Observatory, the Center for Countering Digital Hate, Stanford University, Clemson University, and the University of Washington – serve as cautionary tales and researchers have already indicated that the possibility of legal action has led to chilling effects and self-censorship. See Samuel, V. J. (2025). The State of Independent Technology Research 2025: Power in Numbers. Coalition for Independent Technology Research. https://independenttechresearch.org/wp-content/uploads/2025/08/The-State-of-Independent-Technology-Research-Power-in-Numbers.pdf, Bernstein, A. (2023, March 22). Republican Rep. Jim Jordan Issues Sweeping Information Requests to Universities Researching Disinformation. ProPublica. https://www.propublica.org/article/jim-jordan-information-requests-universities-disinformation, Robins-Early, N. (2024, March 25). Judge dismisses 'vapid' Elon Musk lawsuit against group that cataloged racist content on X. The Guardian. https://www.theguardian.com/technology/2024/mar/25/elon-musk-hate-speech-lawsuit, Spangler, T. (2024, March 25). Elon Musk's X Loses Lawsuit Against Research Group That Reported Rise in Hate Speech, Racist Content on Social Network. Variety. https://variety.com/2024/digital/news/elon-musk-x-loses-lawsuit-against-research-group-hate-speech-racist-content-1235951153

148 Howells, J. (2006) Intermediation and the role of intermediaries in innovation. Research Policy, vol. 35, no. 5, pp. 715–728. https://doi.org/10.1016/j.respol.2006.03.005

intermediaries have already emerged: the DSA Observatory[149] and DSA Research Network[150] serve as hubs for aggregating and producing knowledge on the DSA in general, including its data access provisions. Similarly, the project "Digital Governance for Democratic Renewal" has been facilitating transatlantic exchange for researchers and other stakeholders involved in research data access.[151]

Documentation of researcher experiences with Art. 40(12) DSA and the development of guidance for successful data access applications has also emerged as another important intermediation task.[152] The DSA40 Data Access Collaboratory[153] fulfills this role by providing a tracker[154] to allow for researcher self-reporting and offering application support.[155] Yet, critical gaps remain. As discussed above, there are currently no intermediaries providing infrastructure for performing regular quality checks on the accessed data, or secure, privacy-aware data access modalities, alongside appropriate researcher training. While not aiming to provide infrastructure, the CoCoDa project[156] appears to be taking initial steps to integrate legal and technical expertise to build software supporting researchers on their way to data access.

Furthermore, there is a conspicuous absence of strong researcher associations capable of representing and advocating for researcher interests vis-à-vis enforcement and regulatory bodies—and, ideally, platforms themselves. The Coalition for Independent Technology Research (CITR)[157] is the closest example to date, though its scope far exceeds data access. Other intermediaries could coordinate researchers or create and communicate research syntheses, which is included in the mission statement of the recently established Social Data Science Alliance.[158]

Together, these efforts indicate that the landscape of intermediaries is beginning to take shape, albeit unevenly and with considerable room for development. Importantly, these intermediary roles need not be centralised but actively funded by EU member states or the Union, as their growth will be instrumental in ensuring frictionless and effective data access for risk governance and beyond.

149 https://dsa-observatory.eu/

150 https://www.hiig.de/en/project/dsa-research-network/

151 https://worldprojects.columbia.edu/our-work/research-and-engagement/democratic-renewal/digital-governance

152 The tracking of unsuccessful applications based on 40(4) and the distribution of learnings to a wider researcher community will be an especially critical intermediation task, given that the DSA's data access portal will only publish reasoned requests resulting from successful access applications.

153 https://dsa40collaboratory.eu/

154 The tracker can be found at https://www.soscisurvey.de/DSA40applications/, and aggregate statistics about the submitted information is published at https://dsa40collaboratory.eu/tracker-insights

155 Especially for applications based on Art. 40(4) DSA, DSCs should and will likely provide foundational support and guidance resulting from their ongoing coordination efforts, see supra note 66.

156 https://snsf-cocoda.github.io/

157 https://independenttechresearch.org/

158 https://social-data-science-alliance.org/mission/

Adequate funding

European geoeconomical self-determination requires strong institutions and conditions conducive to innovation. To this end, financial support is essential—both at the organisational level and for specific research projects.

Having outlined the importance of well-resourced DSCs as well as the extent to which researchers need to invest in the build-out of a functional data access ecosystem, it becomes clear that the lack of adequate and sustained support will either lead to a non-functional data access framework, where essential needs are not met, or the degradation of research itself, as valuable resources are diverted to maintain a fragile and inadequate data access regime. To avoid such a scenario, national and super-national budgets[159] need to be mobilised to institutionalise continued financial support for regulatory and enforcement bodies as well as institutions and organisations that fill other key positions in the data access ecosystem.

At the same time research budgets should take into consideration that attempting to answer research questions related to systemic risk through data-intensive approaches that simultaneously meet rigorous standards for data security, privacy and confidentiality will put considerable demands on researcher expertise, applied methodology and technical infrastructure, thereby necessitating significant financial and institutional commitment. This support is essential not only to safeguard the quality and integrity of research but to ensure that attempts at data-driven inquiry into systemic risk do not themselves become a barrier to scientific progress and innovation.

159 For example, EC's proposal for a multi-annual financial framework (MAFF) has earmarked nearly twice the budget for its research programme than available for Horizon Europe in the 2021-2027 period. While this research funding is bundled as part of the European Competitiveness Fund and as such will likely be specifically focused on and subject to increased scrutiny regarding its contribution to innovation and industrial policy, research data access is likely to contribute to both aspects: access-based cross-platform research will have to come up with standardisation techniques that will likely resonate with other legislation like DMA (especially with regard to data portability) and thus create synergies for European companies wanting to offer data transfers from US to EU services. At the same time, research into systemic risk – by both academic and civil society organisations – promises not only to yield openly accessible insights into the safe design of online platforms that will likely be integrated into the design and governance choices of European services providers, but also promote fundamental rights, thereby strengthening the digital single market and making the EU a more attractive market more generally. See Brown, I. (2020). Interoperability as a tool for competition regulation. OpenForum Academy. https://openforumeurope.org/wp-content/uploads/2020/11/Ian_Brown_Interoperability_for_competition_regulation.pdf, Scott, M. (2025, July 21). The Case for Europe's Backing of Digital Civil Society Groups. Tech Policy Press. https://techpolicy.press/the-case-for-europes-backing-of-digital-civil-society-groups, and European Commission (2025). A Dynamic EU Budget for the Priorities of the Future - The Multiannual Financial Framework 2028-2034. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52025DC0570&qid=1753978048542

Final Remarks

The DSA marks a significant change, not just with regards to researcher data access but to platform governance more generally. It challenges long-standing asymmetries in data control and intelligence production as well as non-interoperable systems through its broad transparency mandates, which has led to backlash from actors benefitting from and wanting to maintain the status quo. Thus, the DSA represents not merely a compliance tool but a broader structural intervention into entrenched platform power to assert European digital sovereignty and strengthen the EU's internal market.[160] Its eventual success or failure, especially with regard to researcher data access, is dependent on the active participation of a broad set of stakeholders: from the European Commission, over national authorities, platform companies, and researchers inside and outside academia at the core. Still, early implementation issues clearly demonstrate that the creation of a successful data access regime requires a lot of time as well as work and resource investment from all these stakeholders. This paper has attempted to outline various aspects influencing the realisation of the DSA's ambitious data access regime. If they are addressed through resource investment, stakeholder cooperation and researcher organisation, researcher data access may grow into a solid framework furthering not just knowledge production towards a healthier socio-technical ecosystem but also European innovation and fundamental rights more generally.

160 Whether this leads to a more decentralised digital space or entrenches dominant players – who are best equipped to absorb compliance costs (see supra note 5) – remains an open and contested question.

Imprint

LK Seiling, Clara Iglesias Keller, Jakob Ohme, Ulrike Klinger, Claes de Vreese
Data Access for Researchers under the Digital Services Act: From Policy to Practice

Weizenbaum Policy Paper # 14
Berlin, 09 \ 2025

ISSN 2748-5587 \ DOI 10.34669/WI.PP/14

Weizenbaum-Institut e.V.
Hardenbergstraße 32 \ 10623 Berlin \ Tel.: +49 30 700141-001
info@weizenbaum-institut.de \ www.weizenbaum-institut.de

COORDINATION: Moritz Buchner

With funding from the:
Federal Ministry of Research, Technology and Space
BERLIN
Senate Department for Higher Education and Research, Health and Long-Term Care

weizenbaum institut