DIGITAL SERVICES ACT (DSA)

Preserving fundamental rights when authorities and researchers access data

The successful implementation of the **Digital Services Act** (DSA) is a crucial step to ensure this new framework strengthens the EU digital single market. Particular attention should be paid to **safeguarding the fundamental rights of users and companies alike**.

Article 40 of the DSA lays down the framework that allows authorities and researchers to access a wide range of data held by very large online platforms (VLOPs) and very large online search engines (VLOSEs). The European Commission is expected to publish in the coming months a draft delegated act outlining the technical and detailed conditions and procedures required for accessing such data.

In anticipation of the European Commission's draft delegated act, the Computer & Communications Industry Association (CCIA Europe) offers several recommendations to ensure that the future delegated act safeguards **the protection of the fundamental rights of users and businesses when authorities and researchers seek to access data from VLOPs and VLOSEs, and respects the general principle of proportionality under EU law**.[1] Fundamental rights include users' privacy and the protection of their personal data, the protection of intellectual property, and the freedom to conduct a business, enshrined in the EU Charter of Fundamental Rights. In this respect, we suggest the European Commission considers the following elements in the draft delegated act:

1. Alignment of the delegated act with current legislation

As mentioned in Article 40(13) DSA, the delegated act should outline how the data access process will ensure "the protection of confidential information, in particular trade secrets, and maintaining the security of [VLOPs/VLOSEs'] service". Therefore, the delegated act should impose strict proportionality safeguards regarding the type of information that authorities and researchers may request from VLOPs and VLOSEs to begin with. It should also require those parties to demonstrate they have in place robust systems and mechanisms to protect and prevent the **unauthorised disclosure of confidential company data, data that could undermine the security of systems, or personal data of users, and prohibit the publication of any data obtained through Article 40**. **Nothing in Article 40 should be construed so as to undermine providers' applicable legal obligations or privacy policies.** The draft should also include references to and ensure consistency with requirements in existing legislation, in particular:

- **The General Data Protection Act** (GDPR): Where personal data or mixed data sets are concerned, authorities and researchers' data access requests and subsequent processing should comply with requirements under the GDPR, including the principles of "lawfulness of processing", "purpose limitation," "data minimisation," "storage limitation," and "integrity and confidentiality" under GDPR. Specifically:

[1] CCIA Europe's submission to the call for evidence of the European Commission on the Delegated Regulation on Data Access can be found here.

- CCIA Europe invites the European Commission to consult the European Data Protection Supervisor and issue guidance on which GDPR legal bases companies, researchers, and authorities can rely on to lawfully transfer and process personal data under the GDPR. For companies specifically, it should be clarified that Article 6(1)(c) GDPR (compliance with a legal obligation) is the appropriate legal basis. The delegated act should remedy the lack of granularity of Article 40 DSA, and be sufficiently clear, precise and foreseeable and, in particular, define the purposes of the processing.
- In addition, the range of data subject to those requests and the ways in which authorities and researchers access and further process personal data should be limited to what is strictly necessary to fulfil the request.[2] What might be "useful" does not automatically qualify as "necessary" under the EU data protection acquis.
- Finally, the delegated act should clarify that researchers and authorities are acting as independent "controllers" under the GDPR and must comply with all obligations under the GDPR. This includes complying with all applicable users' rights, as well as implementing appropriate technical and organisational measures at the design stage of the processing to ensure data minimisation, design and implement appropriate security features, notify personal data breaches, conduct a data protection impact assessment, etc. After consulting with stakeholders and analysing the results of the EDMO Pilot Test, the European Commission should provide a range of best practices for each type of data access to help guide authorities and researchers in complying with their technical and organisational obligations.
- At any rate, companies should be able to flag any concerns they may have about a request involving personal data with the competent data protection supervisory authority. We remind the European Commission that VLOPs and VLOSEs have an obligation to consult the competent supervisory authority prior to processing where its data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.

- **The Trade Secrets Directive** (TSD): VLOPs and VLOSEs should be able to decline access requests in exceptional circumstances, when they can demonstrate that they are highly likely to suffer serious damages from such access. This should include situations where researchers or authorities fail to demonstrate that they have taken appropriate technical and organisational measures to preserve the confidentiality and integrity of the trade secrets.

- **The NIS 2 Directive**: Authorities and researchers' handling of data may at times involve the responsibility and liability of VLOPs and VLOSEs with regard to their security obligations under NIS2 (where VLOPs and VLOSEs fall within the scope of application of NIS2). To avoid any undue liability exposure, authorities and researchers should be mandated to inform VLOPs and VLOSEs about security breaches that may affect data disclosed by them. In addition, researchers and authorities should disclose to providers any vulnerability found during the course of their research according to companies' procedures laid down in their vulnerability

[2] European Data Protection Supervisor (EDPS), Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit, 11 April 2017, available here.

handling disclosure programs. In the unlikely event a company fails to acknowledge receipt or does not have an appropriate vulnerability handling disclosure program, authorities and researchers should inform the competent CSIRT. To ensure the responsible handling of vulnerabilities, especially unpatched vulnerabilities, researchers and public authorities should be prohibited from publicly disclosing said vulnerabilities without the permission of the company or the CSIRT involved. Failure to comply with this restriction should result in liability.

2. Organise data access process to uphold fundamental rights

The new DSA data access provision should be balanced with fundamental rights. To achieve this, the delegated act should rely on the following principles:

- **Impose strict proportionality safeguards regarding the type of information that authorities and researchers may request from VLOPs and VLOSEs**.
    - In particular, the burden of proof that the data is requested for the sole purpose of conducting research that contributes to the detection, identification and understanding of systemic risks in the EU, and to the assessment of the adequacy, efficiency and impacts of the risk mitigation measures, should be with the requesting party. Broad, unclear and excessive requests should be rejected.
    - Besides, the delegated act should focus on what the data requests should contain. An explanation of the research objectives would allow platforms to propose appropriate datasets and safeguards.

- **Provide proportionate technical and organisational measures necessary to preserve the confidentiality and security of the data**. While no particular measures should be prescribed, fostering the emergence of best practices and safeguards would be welcome and proportionate with the applicable data being shared.
    - Safeguards should be built within the data access interfaces (such as virtual and physical cleanrooms, CSV files, or APIs) to reduce the risk of data leakage, for example. Similarly, VLOPs and VLOSEs should be able to require registration and monitor the activity on any data access interface to prevent abuse, e.g., in the case of sensitive data.
    - Some safeguards could be useful on a case-by-case basis, depending on the level of security required. These safeguards should include, among others, limited network access, access controls, encryption, restrictions on creating copies, and access control software (with audit logs in case of a breach). Additional measures such as the pre-publication review of research would add an additional layer in certain cases, such as custom datasets.

- **Enable dialogue between parties**. Providers, researchers and authorities should be encouraged to discuss and resolve any technical or organisational challenges either party may be facing when data access requests are made. For instance, the establishment of an independent advisory mechanism or intermediary body could help in balancing the rights of each party when disagreements or uncertainty occur during the review or implementation of any given request. This dialogue may prove useful in various instances:

  - To provide guidance around standardised solutions that ensure that access requests are proportionate to the research goal, well framed given the specific business model involved, and the correct level of aggregation is provided;
  - To avoid access requests evolving into broad enquiries seeking information unrelated to the purpose of the request and endangering users' and businesses' rights;
  - To flag if the requests are not within the scope of detection, identification, and/or understanding of systemic risks and the assessment of mitigation measures and to seek or provide appropriate clarifications or adjustments in scope in this regard or if vetted researcher status is appropriately designated and assigned;
  - To serve as an additional check to ensure consistency across DSCs and limit abuse. In particular, this dialogue would help to resolve situations where platforms may be dealing with multiple overlapping requests in order to try and avoid duplicate or excessive efforts

- **Give time for proper assessment of fundamental rights implications**. If data access should be done within a "reasonable period", it should be explicit that this period be decided on a case-by-case basis with an opportunity for parties to make representations as to what is reasonable. Rushed assessments and disclosures necessarily carry more risks of harm to users' and businesses' rights.

- **Clarify liability in case of breach or misuse**. The researcher or authority in question should be held liable, when necessary, for the data they have requested. The list of damage should cover at least users' privacy breaches and harm to providers (e.g., financial losses or competitive harm).

About CCIA Europe

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

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

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

For more information, please contact:

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