BVDW Statement on the Targeted Public Consultation on the Guidelines on the Trusted Flagger Mechanism under Article 22 of the Digital Services Act

Executive Summary

The German Association for the Digital Economy (*Bundesverband Digitale Wirtschaft e.V.* or BVDW for short) welcomes the European Commission's efforts to promote a consistent and harmonised application of Article 22 Digital Services Act (DSA) across the European Union. A consistent and harmonised application of the mechanism is important to safeguard legal certainty, procedural safeguards and fundamental rights throughout the European Union.

BVDW supports the recognition that the trusted flagger mechanism can contribute to a more effective and reliable handling of notices concerning illegal content, while preserving providers' responsibility to conduct their own independent assessments. To achieve this, the designation process must ensure a high degree of reliability while remaining proportionate, transparent and accessible to qualified applicants. In this context, BVDW also welcomes the case-by-case assessment of applications, as different categories of illegal content raise distinct legal, factual and technical challenges.

BVDW further supports the Commission's recognition that a broad range of entities – including industry associations, civil society organisations and other qualified private actors – may qualify for trusted flagger status, as a diverse ecosystem strengthens the quality, credibility and balance of enforcement. At the same time, the final Guidelines should not introduce additional criteria for private entities, commercial actors or industry associations beyond those set out in Article 22(2) DSA (cf. para 32(b) and para 59), which does not distinguish between public, non-profit and commercial entities. The mere commercial nature of an applicant should therefore not be treated as an indicator of lower trustworthiness. Recognition may instead be conditioned on demonstrated notice quality and compliance with minimum content requirements, thereby mitigating the risk of automated or error-prone mass notifications. BVDW also welcomes the clarification that financial support from online platforms does not automatically call into question an applicant's independence; the relevant assessment should focus on whether such funding is capable of impairing the applicant's ability to act independently and objectively.

Beyond these substantive aspects, the draft Guidelines provide valuable clarification on several procedural elements of the designation and notification process and should be understood as an overarching framework for trusted flaggers, providers and Member States alike. In the interest of legal certainty and a level playing field within the Digital Single Market, Member States should refrain from imposing additional national obligations that go beyond the interpretation of Article 22 DSA reflected in the Guidelines. While formally non-binding, the Guidelines are likely to serve as a key reference point for regulators and auditors and may, in practice, become de facto compliance benchmarks. They should therefore focus on supporting a uniform interpretation of Article 22 DSA without creating obligations beyond those established by the Regulation itself.

Against this background, several provisions – particularly in Chapter 5 – appear to go beyond the requirements of Article 22 DSA by setting out detailed technical and organisational expectations. While providers must ensure priority treatment of trusted flagger notices without undue delay, the DSA does not prescribe specific technical or operational arrangements. The final Guidelines should therefore adopt a more clearly outcome-based approach, preserving flexibility for providers to implement appropriate processes in light of their size, resources, risk profile and operational realities. Given the diversity of services covered by the DSA, a one-size-fits-all approach would be neither practical nor proportionate. A stronger emphasis on proportionality, flexibility and legal certainty would support consistent implementation across the Digital Single Market while accommodating different platform types and business models.

Statement

Overall Assessment and General Comments

BVDW welcomes the opportunity to provide comments on the European Commission's draft Guidelines on the trusted flagger mechanism under Article 22 of Regulation (EU) 2022/2065 (Digital Services Act, "DSA").

At the outset, BVDW would like to express its support for the Commission's objective of promoting a consistent and harmonised application of Article 22 DSA across the European Union. The trusted flagger mechanism can contribute to a more effective, reliable and rights-sensitive handling of notices concerning illegal content, provided that it is implemented in a proportionate manner, reflecting the realities of the diverse digital economy.

Additionally, BVDW welcomes the explicit invitation addressed to Digital Services Coordinators ("DSCs") to refer to the Guidelines when implementing and enforcing Article 22 DSA. A harmonised approach in this area is particularly important in order to avoid fragmentation between Member States, divergent national practices and legal uncertainty for trusted flaggers, applicants, online platforms and other stakeholders. In this respect, para. 17 of the draft Guidelines is a helpful starting point.

BVDW further welcomes the clarifications in para. 17 and para. 22 that the Guidelines are not legally binding. The interpretation of Article 22 DSA ultimately remains within the jurisdiction of the Court of Justice of the European Union. This clarification is essential. However, several provisions of the current draft Guidelines are formulated in a manner that could be understood as setting concrete compliance requirements rather than providing interpretative guidance. This creates uncertainty as to the intended legal status and normative weight of the recommendations contained in the draft Guidelines.

This concern is particularly relevant because, although the Guidelines are formally non-binding, they are likely to play an important role in the practical interpretation and enforcement of Article 22 DSA by DSCs, national authorities, auditors and other relevant stakeholders. In practice, recommendations included in Commission guidance may become de facto compliance benchmarks. The final Guidelines should therefore avoid wording that could be understood as creating legal obligations beyond the DSA itself. Against this background, BVDW recommends that the Commission clarifies that the Guidelines are intended to support a uniform application of Article 22 DSA and do not establish additional legal obligations beyond those laid down in the Regulation. This is particularly relevant with regard to the legal basis of the Guidelines. Article 22(8) DSA empowers the Commission to issue guidelines to support providers of online platforms and DSCs in the application of Article 22(2), (6) and (7) DSA. This mandate is also reflected in para. 9 and para. 20 of the draft Guidelines. By contrast, Article 22(8) DSA does not empower the Commission to prescribe detailed additional requirements under Article 22(1) DSA, relating to specific technical or organisational measures to be implemented by providers of online platforms. Providers and operators of online platforms are free to implement the technical and operational requirements in a way that works in their independent systems.

Guidance provided by the Commission on Article 22(1) DSA should therefore exclusively be labelled as non-binding, illustrative and ancillary to the statutory obligation to provide priority treatment to notices submitted by trusted flaggers. It should not be presented as prescribing specific compliance measures, technical architectures or organisational models.

It should also be recognised that the practical relevance of the trusted flagger mechanism differs significantly across providers. Many online platforms (particularly those not classified as VLOPS) currently receive only a very limited number of trusted flagger notices, while others have not received any notices whatsoever. Therefore, the final Guidelines should remain proportionate. The implementation of Article 22 DSA should furthermore remain sufficiently flexible to take into account the actual risk profile, scale and operational realities of different services.

Against this background, the following comments focus primarily on Chapters 3, 4 and 5 of the

draft Guidelines, as well as on selected cross-cutting issues that are particularly relevant for the practical operation of the digital economy regarding a coherent implementation of the trusted flagger system.

Chapter 3: Awarding the Trusted Flagger Status

BVDW supports the Commission's approach of limiting trusted flagger status to entities that fulfil the three cumulative requirements set out in Article 22(2) DSA, namely particular expertise and competence in identifying, detecting and reporting illegal content, independence from providers of online platforms, and the diligent, accurate and objective performance of notice-submission activities. These criteria are essential to safeguard the integrity, credibility and effectiveness of the trusted flagger mechanism. Given that trusted flagger notices benefit from priority treatment, the designation process must ensure a high degree of reliability while remaining proportionate, transparent and accessible to qualified applicants.

BVDW also welcomes the Commission's recognition that applications should be assessed on a case-by-case basis. Different categories of illegal content raise very different legal, factual and technical challenges.

Furthermore, BVDW explicitly support the Commission's recognition that a broad range of entities may qualify for trusted flagger status, including industry associations, civil society organisations and other qualified private entities. A diverse trusted flagger ecosystem is essential to ensure that the framework benefits from a wide range of expertise, practical experience and perspectives across different sectors, services and types of illegal content. Broad participation helps to strengthen the quality and credibility of notices, promotes balanced and proportionate enforcement, and reduces the risk of over-reliance on any single stakeholder group.

At the same time, the final Guidelines should not discriminate and provide further criteria for assessing private entities, commercial actors and industry associations than those requirements set out in Art. 22 (2) DSA (cf. Para 32 b) and para 59. Article 22(2) DSA does not distinguish between public, non-profit and commercial entities or justify any higher degree of scrutiny.

Moreover, the mere commercial nature of an applicant should not be regarded as an indicator of lower trustworthiness under Article 22 DSA. Instead, the Guidelines should emphasise that recognition of private entities, including commercial rightsholders and their representatives, may be conditioned on demonstrated notice quality and compliance with minimum content requirements, thereby mitigating the risk of excessive volumes of automated or error-prone notifications that could undermine the effectiveness of the trusted flagger system.

Finally, BVDW welcomes the clarification that financial support from providers of online platforms does not automatically call into question an applicant's independence. A purely formalistic approach would risk excluding highly qualified expert organisations that rely on mixed funding models. The assessment should instead focus on whether the nature, scope and conditions of the funding are capable of impairing the applicant's ability to act independently, objectively and without undue influence. This also underlines the aforementioned point for additional criteria for trusted flagger applications from private interest groups.

Chapter 4: Notification of Trusted Flaggers to the Commission

BVDW generally welcomes the establishment of clear, proportionate and harmonised procedures governing the notification of trusted flaggers and the operation of the trusted flagger database. In particular, BVDW welcomes the obligation set out in para. 63 for DSCs to inform the Commission without undue delay about newly designated trusted flaggers. This helps to ensure that providers of online platforms are able to verify the identity and designated area of expertise of trusted flaggers at an early stage and contributes to the transparency and reliability of the mechanism.

At the same time, the draft Guidelines leave important questions unanswered. Most notably, it remains unclear at which precise point the obligations of providers of online platforms under Article 22(1) DSA become applicable. The current draft does not clarify whether notices submitted by a trusted flagger must already receive priority treatment before that entity has been

formally entered into the public database. From the perspective of the digital economy, a clear and legally certain trigger is required. The obligation to provide priority treatment should arise only once the relevant trusted flagger has been recorded in the publicly accessible and machine-readable database and can be verified by providers of online platforms. Only such an approach provides a practical and objective basis for compliance and avoids legal uncertainty for both providers and trusted flaggers. Of course, providers of online platforms should remain free to voluntarily prioritise notices from prospective or non-designated trusted flaggers where this is deemed appropriate based on their own risk assessments, operational experience, or established cooperation mechanisms. However, such voluntary practices should not alter the legal trigger established by Article 22 DSA, nor create an expectation that the statutory obligations associated with trusted flagger status apply before formal designation and registration in the public database.

Closely linked to this issue is the question of how providers of online platforms become aware of newly designated trusted flaggers and subsequent status changes. While Article 22(5) DSA and the draft Guidelines provide for a publicly accessible database, neither the DSA nor the draft Guidelines require the Commission to actively notify providers of new designations, changes in scope, suspensions or revocations. Given that the trusted flagger status directly triggers obligations for providers under Article 22 DSA, the introduction of a standardised notification mechanism would significantly help improve legal certainty and operational reliability. The final Guidelines should therefore encourage the Commission to automatically inform providers of online platforms of relevant updates to the database, including new designations, changes to the designated area of expertise, suspensions and revocations. Such an approach would facilitate the timely and accurate integration of status changes into providers' internal review and moderation processes.

The functioning and maintenance of the database also deserves further attention. para. 68 rightly requires that inaccuracies and technical issues affecting the database be reported without delay. However, the provision primarily refers to DSCs and trusted flaggers. Providers of online platforms are among the primary users of the database and are an important group to identify technical errors, inconsistencies or security-related issues. The final Guidelines should therefore explicitly include providers in their database reporting system. Ensuring that all relevant stakeholders can contribute to the identification and resolution of database-related problems would strengthen the integrity, reliability and long-term functionality of the system.

Additional clarification is also required regarding the interaction between para. 64 and para. 66 concerning the processing of personal data. para. 64 provides for the transmission of certain information relating to trusted flaggers, whereas para. 66 clarifies that no personal data should be transmitted. While these provisions may be interpreted as permitting the disclosure of information relating to the trusted flagger organisation itself, but not personal data concerning individual natural persons, the interplay between the two provisions remains insufficiently clear. To avoid uncertainty in practice, para. 66 should explicitly clarify that the prohibition on transmitting personal data also applies to the information referred to in para. 64. Alternatively, the Guidelines could clarify that no personal data may be transmitted except for information expressly required under Article 22(4) DSA and specified in para. 64. Such clarification would improve legal certainty and facilitate a consistent application of the Guidelines in compliance with data protection requirements.

Chapter 5: Submission and Processing of Notices

BVDW welcomes the Commission's clarification that trusted flaggers do not determine whether content should be removed or restricted and that providers of online platforms remain responsible for conducting their own careful and independent assessments of notified content. This clarification, reflected in para. 83, is important for preserving the allocation of responsibilities under the DSA, ensuring legal certainty and safeguarding fundamental rights.

This clarification is fully consistent with the structure of Article 22 DSA, which is limited to requiring providers of online platforms to give priority treatment to notices submitted by trusted flaggers and to process such notices without undue delay. The provision does not prescribe how providers must organise their internal processes or which technical tools they must deploy.

Against this background, several provisions of Chapter 5 appear to go beyond interpretative guidance and towards prescribing particular implementation measures.

BVDW supports the objective of ensuring the reliable verification of trusted flaggers and the authenticity of the notices they submit. Effective verification mechanisms are important for maintaining the integrity and trustworthiness of the trusted flagger mechanism. However, the references in para. 70 and para. 78(a) to multi-step verification procedures, two-factor authentication systems and secure digital certifications appear relatively prescriptive and could be interpreted as favouring a particular implementation model. Article 22 DSA itself does not prescribe specific authentication requirements or technical verification methods. The appropriate level and form of verification may differ depending on the provider's risk profile, technical architecture and operational context. It furthermore does not provide flexibility for potential future technology developments or new authentication processes. For this reason, the final Guidelines would benefit from a more outcome-oriented approach focused on ensuring the reliable verification of trusted flaggers and their notices, while preserving sufficient flexibility for providers to determine the most appropriate technical means of achieving that objective. To avoid any uncertainty regarding the intended legal effect of these recommendations, it would also be helpful to clarify that the measures referred to in para. 70 and para. 78(a) are examples of good practices rather than expected or mandatory implementation requirements.

Para. 71 and para. 72 further refer to standardised onboarding procedures and a central electronic contact point. These measures may be useful in practice but should be framed as possible implementation options rather than expected compliance requirements. The same applies to the requirement in para. 72 that such contact points be adequately staffed. Article 22 DSA does not prescribe a specific organisational model for providers.

Para. 35 states that providers should use the harmonised taxonomy of illegal content under Implementing Regulation (EU) 2024/2835 when taking technical and organisational measures under Article 22(1) DSA. It also considers that providers should use those types when taking the technical and organizational measures to which Art. 22 refers (para. 75). This reference should not be understood as creating a factual obligation to incorporate those granular categories into platforms' own notice forms, interfaces or internal workflows. Neither Article 16 nor Article 22 DSA provides a legal basis for prescribing the concrete design of notice forms. The decisive criterion should be whether notices can be effectively, clearly and reliably processed.

Para. 76 states that compliance with Article 22(1) DSA requires technical and organisational measures going beyond Article 16 DSA and, in the Commission's view, includes dedicated contact points and "dedicated channels" for trusted flagger notices. This should be clarified. Article 22(1) expressly refers to notices submitted through the Article 16 mechanism. The Guidelines should therefore not create the impression that providers are required to establish separate or exclusive channels for trusted flaggers.

Para. 78(b) provides that providers should grant trusted flaggers access to an API to facilitate the submission of notices and enable standardised retrieval of information. Similarly, para. 88 refers to retrospective access to information, preferably via API and in machine-readable format. APIs may be useful in certain contexts, particularly where high volumes of notices are submitted. However, Article 22 DSA does not impose an obligation to provide API-based access. Such access should therefore be framed as a voluntary implementation option or good practice, not as a standard requirement.

Para. 78(c) states that providers should allow content "of any form" to be notified as illegal content. This wording is overly broad and should be clarified. To avoid legal uncertainty and an unintended expansion of the scope of the requirements, the Guidelines should use a more precise formulation, for example by referring to user-generated content where appropriate.

BVDW also welcomes the flexibility reflected in para. 86, according to which trusted flagger notices should, on average, be processed faster than other notices concerning the same type of illegal content. However, the reference to average processing times may be misleading, as

individual complex cases can distort average values. A reference to median processing times would provide a more robust and comparable indication of typical processing durations.

Para. 87 states that providers should establish dedicated, well-functioning and adequately staffed channels for processing trusted flagger notices and consider available technologies to avoid unnecessary delays. While efficient processing is important, the Guidelines should not prescribe dedicated teams or channels as a specific organisational model. Compliance with Article 22 DSA should be assessed by reference to effective prioritisation and timely processing, not by whether a provider has implemented a particular internal structure.

Para. 88 raises additional concerns insofar as it suggests that providers should facilitate retrospective access to information relating to notices submitted by trusted flaggers. To the extent this is intended to support trusted flaggers' own reporting obligations, the provision risks shifting those obligations onto providers' IT systems and operational resources. Any such information access should be subject to proportionality, confidentiality and data protection requirements and should be framed as voluntary cooperation rather than a legal obligation.

Finally, para. 84 and para. 89 raise concerns regarding prioritisation. BVDW agrees that the most severe and urgent cases, in particular those involving threats to life or safety, should be addressed promptly regardless of whether the notice was submitted by a trusted flagger or another user. However, the Guidelines should avoid creating multiple layers of prioritisation. If too many categories or criteria are treated as requiring priority, prioritisation risks losing its practical function. In particular, the expectation in para. 89 to ensure balanced processing times across different types of illegal content may create an additional prioritisation layer among trusted flagger notices that is not provided for in the DSA.

The final Guidelines should therefore adopt a clearly outcome-based approach. Providers should be required to ensure effective priority treatment of trusted flagger notices and timely, careful decision-making. However, they should retain flexibility as to the technical, procedural and organisational means used to achieve that outcome, taking into account their size, resources, technical architecture, business model, risk profile and the volume of trusted flagger notices they actually receive. Given the diversity of services covered by the DSA, a one-size-fits-all approach would be neither practical nor proportionate. The final Guidelines should therefore accommodate different operational realities while ensuring consistent implementation of Article 22 DSA across the Digital Single Market.

Bundesverband Digitale Wirtschaft (BVDW) e.V.

The German Association for the Digital Economy (BVDW) is the advocacy group for companies that operate digital business models or whose value creation is based on the use of digital technologies. With its members from the entire digital economy, the BVDW is already shaping the future today through creative solutions and state-of-the-art technologies. As a catalyst, guide, and accelerator for digital business models, the association relies on fair and clear rules and advocates for innovation-friendly framework conditions. BVDW always keeps an eye on the economy, society, and the environment. In addition to DMEXCO, the leading trade fair for digital marketing and technologies, and the German Digital Award, the BVDW also organizes the CDR Award, the first award ceremony in the DACH region for digital sustainability and responsibility, as well as a variety of specialized events.

Author: **Fabian Miller**, Junior Public Affairs Manager – Data Society, miller@bvdw.org

www.bvdw.org

Imprint

Place and Date of Publication	Berlin, 10 July 2026
Published by	Bundesverband Digitale Wirtschaft (BVDW) e.V. Obentrautstraße 55, 10963 Berlin, +49 30 2062186 - 0, info@bvdw.org, www.bvdw.org
Executive Board § 26 BGB President	Carsten Rasner Dirk Freytag
Vice Presidents	Thomas Duhr, Anke Herbener, Corinna Hohenleitner, Dr. Moritz Holzgraefe, Julian Simons, Björn Kaspring
Contact	politik@bvdw.org
Association Register Number VR 42449 B	Amtsgericht Charlottenburg
Legal Notice	All information and data contained in this publication have been carefully researched and reviewed by the German Digital Industry Association (Bundesverband Digitale Wirtschaft – BVDW) e.V. This information is provided as a service by the Association. Neither the BVDW nor the companies involved in the preparation and publication of this work assume any liability for the accuracy, completeness or timeliness of the information provided.
	The contents of this publication and/or references to third-party content are protected by copyright. Any reproduction of information or data, in particular the use of texts, excerpts of texts, images or other content, requires the prior consent of the German Digital Industry Association (Bundesverband Digitale Wirtschaft – BVDW) e.V. or the respective rights holders (third parties).

EU Transparency Register Number: 479540331468-69 German Lobby Register Number: R000257