Position

28.10.2025
Philipp Hagen, Director Legal Affairs & Data Privacy, hagen@bvdw.org
Fabian Miller, Junior Public Affairs Manager, miller@bvdw.org

Position paper on the EDPB Consultation regarding the Guidelines 3/2025 on the interplay between the DSA and the GDPR

The German Association for the Digital Economy (BVDW) e. V. is the industry association for companies that operate digital and data-driven business models or whose value creation is based on the use of data and digital technologies. With its members from the entire digital economy value chain, BVDW and its members are already shaping the future today through creative solutions and state-of-the-art technologies. With more than 600 members ranging from large and small digital enterprises to agencies and publishers BVDW represents the interests of the digital economy vis-à-vis policymakers and society. Through its broad network of experts, the association provides data-driven insights, facts, and guidance on one of the most important fields shaping the future.

BVDW welcomes the EDPB's initiative to clarify the complex interplay between the GDPR and the DSA through the publication of dedicated guidelines. We appreciate the opportunity to contribute to this important consultation and would like to thank the EDPB for allowing stakeholders to provide input. Given the far-reaching implications of both frameworks for digital business models, advertising ecosystems and innovation in Europe, it is essential that the guidelines ensure coherence, proportionality and practical applicability. Against this background, BVDW would like to share a number of observations from the perspective of the digital economy.

1) General Remarks

BVDW acknowledges the EDPB's important role in promoting the coherent application of data protection rules across the EU. Companies operating under both the DSA and the GDPR face significant compliance challenges arising from overlapping obligations, evolving enforcement structures and parallel oversight by different authorities. These challenges are particularly important for Medium-sized Enterprises or Mittelstand companies, which constitute a large number of the digital economy. Mittelstand companies form the backbone of Europe's innovation and competitiveness. Clear, predictable, and practicable guidance is therefore essential to ensure legal certainty, compliance efficiency, and a level playing field throughout the Single Market.

While the draft guidelines aim to clarify this interplay (para 1), they remain at times, highly abstract, providing limited practical orientation for organisations implementing both frameworks. For the industry, this level of abstraction is not a theoretical problem but a direct practical barrier to compliance. Companies require clear, actionable instructions and legal certainty. In several areas, the drafting of the guidelines can potentially blur institutional boundaries and create residual uncertainty (e.g. para 46, 47, 62, 89), a tendency that has already raised concerns regarding the interpretation of competencies in the past. While the guidelines rightly focus on GDPR-relevant processing, they necessarily intersect with DSA-related interface issues (e.g. paras. 44–47, 89–96). This is legitimate and valuable. However, the absence of clear signposting to the respective remit of the Digital Services Coordinators (DSCs) will create uncertainty for companies as to which authority's expectations prevail in practice and whether the EDPB guidelines reflect the DSC and EBDS views. Having long advocated for strong cross-regulatory collaboration, BVDW regrets this missed opportunity.

To meet their intended purpose, the guidelines should prioritize instructions for practical implementation. From the perspective of the digital economy, this calls for more concrete examples and implementable guidance tailored to platform operations, and for template procedural notes and FAQs for companies, and specifically for Mittelstand companies and startups developed with DSCs to lower compliance barriers. Prior consultation to explicitly define the DSC's complementary role is essential to prevent regulatory overlap and ensure coherent enforcement across both frameworks.

The following sections address specific areas of the draft and invite alignment with the DSA's underlying objectives and operational realities.

2) Specific Remarks on the Draft Guidelines

Against this backdrop, we offer the following observations with a view to enhancing clarity where it matters most. In places, the drafting blurs institutional boundaries or may be read as touching on DSA-specific matters, even where a GDPR nexus exists. The point is not one of abstract mandate, but of practical clarity for providers operating under coordinated supervision across both regimes.

a. Deceptive patterns – scope and institutional clarity

This section addresses deceptive design as it crystallises the need for precise scoping and coordinated supervision. We recognise the EDPB's essential role in clarifying interface patterns where a clear GDPR nexus exists. As set out in para. 44, principles of fairness, transparency, and data protection by design and by default are fundamental whenever interface patterns affect or condition the processing of personal data. Para. 44 therefore delineates the appropriate remit. However, the concept of "deceptive design" or "Dark

Patterns" is far broader than its data protection implications. As BVDW we have detailed in a dedicated position paper on this topic, that these "Dark Patterns" are already addressed by a complex landscape of EU legislation, including the specific prohibition in Art. 25 DSA, the general rules of the Unfair Commercial Practices Directive (UCPD), and prohibitions on manipulation in the AI Act (Art. 5). The GDPR, while relevant for manipulative consent mechanisms, governs only a fraction of this multifaceted debate.

Paragraphs 46–47 introduce additional examples such as "addictive designs", "infinite scrolling" and "infinite streaming". The examples provided in relation to dark patterns suggest that design patterns like infinite scroll and streaming features could amount to GDPR violations if they indirectly result in data disclosure, and it is unclear which would fall under the DSA and which would fall under the GDPR. These examples are drawn from a broader DSA and Digital Fairness debate. They relate more closely to consumer protection or the systemic design obligations under Art. 25 DSA. Furthermore, the EDPB's analysis of 'addictive behaviour' is a particular concern, as this is a highly complex scientific topic, and the guidelines provide no objective foundation or evidence for this analysis. Indeed, there currently is no common definition of "Dark Patterns" or "deceptive design", neither in the framework of the GDPR, the DSA or the continuing discussions on the Digital Fairness Act. BVDW agrees that specific practices involving manipulation or clear consumer deception, must be addressed and prevented, as the industry also clearly rejects in our position paper. However, these genuinely harmful instances with manipulation at its core, represent only a very small subset of digital interface design. The current broad-brush approach in the draft guidelines contributes to a problematic conceptual blurring. It creates a risk where legitimate and common design practices, necessary user guidance, or standard marketing techniques are unfairly conflated with actual deceptive patterns.

Similar coordination sensitivities arise elsewhere in the draft where substantive DSA matters appear to be engaged, including the assessment of technologies for detecting illegal content (paragraphs 15–16) and various statements on advertising, recommender systems and risk assessments (paragraphs 52, 67, 75, 76, 78, 86, 87, and sections 2.3 and 2.7). While the EDPB is legally entitled to address these topics from a GDPR perspective, broad definitional treatment risks overlap and the perception of pre-empting DSC interpretations. Therefore, BVDW calls on clarity on the topic of "Dark Patterns" as a cross-horizontal issue with additional definition guidelines that give practical implementation guidance to companies operating in the European Union. To ensure the final guidelines are coherent and practically aligned, we urge the EDPB to actively engage with the EBDS, national DSCs, and the EU Commission, ensuring their perspectives are fully integrated. This collaborative approach would honour the principles of the Helsinki statement and

mirror the successful inter-regulatory dialogue the EDPB established for its DMA and AI Act guidance.

b. Age Assurance and the Risk of Undermining Effective Protection

Regarding age-assurance measures under Art. 28 DSA and the guidelines from the Commission on the protection of minors from July 2025, the core challenge is to implement this obligation without discarding fundamental data protection principles. We therefore agree with the EDPB's starting point of the explicit emphasis on a risk-based approach, as well as on necessity, proportionality and privacy by design, to provide the correct foundation. These principles are essential for developing targeted, privacy-preserving solutions. As part of this, we urge the EDPB to provide the necessary legal certainty that biometric processing for the sole purpose of age estimation – as distinct from unique identification – does not fall under the scope of Article 9. Accordingly, data-protection standards should be interpreted and operationalised in a way that is practicable and coherent with providers' obligations under the DSA; absent such alignment, compliance will gravitate toward form over substance.

This could force reliance on lighter-touch measures that are easily circumvented, thereby failing both the objective of the DSA and the protection of minors. The DSA and GDPR must be applied coherently, not in opposition. The draft rightly notes that Article 28(1)–(2) DSA can serve as a legal basis under Article 6(1)(c) GDPR. The final guidelines must therefore confirm that this legal basis allows for the processing that is strictly necessary and proportionate to meet that specific legal obligation, evaluated on a calibrated, case-by-case basis. This enables a truly risk-based approach: while low-risk, general-audience services can use lighter measures, high-risk services must be permitted to deploy more robust safeguards. This also aligns with the European Commission's Article 28 DSA guidance, which expects platforms to enable age-stratified experiences – an outcome that, in practice, presupposes reliable knowledge of an age band. Therefore, the EDPB's restrictive approach in paragraph 94, which discourages storing an age range, is operationally problematic. It prevents the application of differentiated settings for different age groups (e.g., younger vs. older teens) as supported by the European Commission Art.28(4) DSA guidelines and would lead to more disruptive, excessive processing from repeated verifications, undermining data minimization.

c. Advertising and Article 22 GDPR

A key source of potential legal uncertainty is the reading of para. 62 of the draft guidelines, which may be understood as suggesting that the requirements of Article 26(1) DSA could, in certain circumstances, trigger Article 22(1) GDPR for the selection and presentation of

advertising. While the intention to protect vulnerable data subjects is legitimate, applying the threshold of “legal effects or similarly significant effects” to the automated delivery of an advert risks extending Article 22 beyond its intended scope.

We assert that the mere act of presenting an advertisement, regardless of the level of profiling involved, does not constitute a legal effect, nor does it reach the high bar of "similarly significantly affecting" a data subject. To illustrate this high bar, it provides concrete examples such as the "automatic refusal of an online credit application or e-recruiting practices without any human intervention." These examples clearly demonstrate the legislator's intent: Article 22 is designed to govern decisions that fundamentally alter a person's life, legal standing, or access to essential opportunities – unlike credit scoring, insurance risk assessment, or job application filtering. Even the Article 29 Working Party guidelines state that in many typical cases, targeted advertising would not have a significant impact on individuals, but this is not reflected in the guidelines. The EDPB should clarify, that in most instances, advertising will not qualify as a decision under Art. 22(1) GDPR. It lacks legal effect, and it typically does not significantly affect the individual in a comparable manner. Most ad-tech providers operate on pseudonymised data, making the inference of individual vulnerabilities highly unlikely and often contrary to their compliance obligations. As a member of IAB Europe, we note that our position aligns with IAB Europe’s analysis on this point.

We recommend that paragraph 62 be refined to (i) state that standard advertising practices ordinarily fall outside Article 22(1) GDPR, and (ii) set out narrow, clearly defined exceptional cases where Article 22(1) could apply, supported by factor-based examples and aligned with established EU frameworks. This approach preserves robust protections for users while providing businesses with clear, workable guardrails for compliant ad-delivery transparency.

d. Recommender Systems

BVDW acknowledges the EDPB’s attention to recommender systems (paras 80–88 of the guidelines) and their potential to affect users’ access to information. Recommender algorithms enable the discoverability of relevant content, the personalization of services, and the efficient allocation of digital advertising.

The BVDW agrees that recommender systems should operate transparently and in compliance with data-protection principles whenever personal data are processed. However, we are concerned by the guidelines’ suggestion that recommender systems could trigger Article 22 of the GDPR (para 84). The mere presentation of content does not meet the high legal threshold of a 'legal or similarly significant effect,' which is reserved for decisions with profound, lasting, or discriminatory impacts. Similarly, the guidelines'

definition of 'profiling' is so expansive it risks capturing basic, necessary contextualization for language or region, which has no such significant effect on the individual. Besides, parts of the draft guidelines appear to imply that Very Large Online Platforms (VLOPs) and Search Engines (VLOSEs) must present profiling-based and non-profiling options equally or refrain from using profiling by default before explicit user selection. Such an interpretation would exceed the scope of the DSA and could unintentionally constrain legitimate service design and user-experience optimization.

Article 27 and 38 DSA do not mandate identical presentation, default parity, or interface symmetry between different recommender options. Imposing such equality would amount to an additional "choice architecture" obligation not foreseen by the DSA, thereby creating unnecessary friction for both users and providers.

From the perspective of the BVDW, proportionality and user relevance should guide interpretation:

- Profiling-based recommendations are lawful and valuable when users have meaningfully consented, or another valid legal basis applies.
- Non-profiling alternatives should be accessible and understandable but not required to be highlighted or presented identically to personalized options.
- Platforms should retain design autonomy to integrate these options in a way that fits their service logic, provided that transparency and user control are ensured.

The BVDW therefore recommends that the final guidelines clarify that Articles 27 and 38 DSA do not require equal or default-neutral presentation of profiling and non-profiling options; reiterate that legitimate user-experience design, including default recommendations, is permissible where based on a valid legal ground and consistent with fairness and transparency; and encourage risk-based differentiation, allowing stricter presentation requirements only where recommender outcomes may significantly affect users' rights (e.g. exposure to harmful or illegal content).

3) Conclusion

To be effective, the final guidelines must strike a difficult but essential balance: they must uphold the high standards of the GDPR without inadvertently neutralizing the core protective and functional obligations of the DSA. The digital economy requires legal certainty, which can only be achieved through clear, practical guidance that respects the distinct institutional roles of the EDPB and the Digital Services Coordinators. We have highlighted key areas – particularly regarding deceptive design, age assurance, the scope

of Article 22 GDPR, and recommender systems – where this clarity and inter-authority alignment are most critical.

We urge the EDPB to integrate the perspectives of the EBDS, national DSCs, and the Commission to ensure a truly coherent, proportionate, and workable framework. The BVDW remains committed to a constructive dialogue to help achieve a digital single market that is both innovative and safe for all users.