bitkom

Position Paper

October 2025

Bitkom on the EDPB´s Guidelines 03/2025 on the interplay between the DSA and the GDPR

Summary

Bitkom welcomes the European Data Protection Board's (EDPB) initiative to provide guidance on the interplay between the Digital Services Act (DSA) and the General Data Protection Regulation (GDPR). Legal clarity in this area is essential to effectively implement the obligations of both frameworks, safeguard users' rights, and foster continued innovation in the digital economy.

Bitkom would have welcomed closer coordination with the Digital Services Coordinators in the preparation of these guidelines. The EDPB´s unilateral approach creates a twofold problem: it is inconsistent with the spirit of cross-regulatory cooperation championed in the Helsinki statement, and it fundamentally undermines legal certainty by omitting the perspective of the authorities responsible for the DSA's implementation and who may be better placed to define some of the terms used by the EDPB.

While the draft guidelines provide a valuable starting point, they raise concerns regarding legal certainty, operational feasibility, and the overall balance between data protection, user safety, and innovation. In their current form, the guidelines lack the comprehensive clarity needed to be fit-for-purpose for all stakeholders. It also places disproportionate emphasis on data protection risks, while the broader objectives of the DSA—such as user safety, systemic risk mitigation, and platform integrity—are not given adequate consideration. Bitkom therefore strongly encourages the EDPB to adopt a proportionate and risk-based approach that reflects the operational realities of complying with the DSA and the measures required to achieve online safety.

1. Automation and content moderation

Automation plays an indispensable role in content moderation, enabling scalable and effective enforcement against illegal or harmful content. The expectation in the draft guidelines that providers should always consider less intrusive means should be interpreted in a practical manner, recognising that certain processing activities are in fact strictly necessary to ensure effective content moderation and online safety. In practice, automated tolls are an effective way to manage the enormous volume of content that circulates on digital platforms. Bitkom would like to be provided with further clarity and the recognition in the Guidelines that any content moderation techniques will require the processing of personal data. To this end, 'legitimate interest' (Art. 6(1)(f) GDPR) is an available and appropriate legal basis, as the Guidelines partially recognise. We would encourage the EDPB to clarify that this interest is not limited to illegal content but also necessarily extends to addressing violations of terms of service, which serves a broader societal interest in user safety.

Equally concerning is the broad interpretation of Article 22 GDPR, which appears to treat most automated enforcement decisions as automated decision making (ADM). This interpretation is excessive and disregards operational practices such as risk assessment and DPIAs where required. It also imposes a new, higher threshold for this legal basis (para 21) that is not supported by the cited case law (C-817/19), which concerns Charter limitations, not the criteria for Article 6(1)(c) GDPR. This interpretation also misaligns with Recital 41 of the GDPR, and we encourage the EDPB to ensure the guidelines do not unintentionally raise the bar for relying on legal obligation for DSA compliance.

The Guidelines should clarify that voluntary investigations by platforms to detect and remove illegal content will unlikely be considered ADM under Article 22 GDPR. Most proactive moderation decisions do not have the kind of legal or significant effects contemplated by the GDPR in its provisions on automated decision-making (Article 22 GDPR), the accompanying recitals in the GDPR and the Article 29 Working Party (i.e., the body preceding the EDPB) guidelines on ADM. For most types of content these voluntary own-initiative investigations and any personal data processed will not meet the threshold for ADM as content will be of an innocuous nature, and personal data processing will be only a limited part of these investigations.

Regarding notice and action mechanisms, these must protect users' personal data while ensuring that providers can effectively respond to reports of illegal content. The Guidelines reference data minimisation in this section 2.2.1, however the Guidelines should also consider other data protection principles like accuracy and purpose limitation in relation to notice and action mechanisms and take into account that these are given equal importance under the GDPR. Anonymous reporting should be allowed in certain cases, but providers also need flexibility to verify notifier identities where reasonably necessary to prevent abuse or assess legality. The DSA itself contains wording on these points which allow providers to collect further identification information. The Guidelines should emphasise enabling privacy-preserving safeguards that still allow responsible handling of abuse and illegal content.

2. Data Minimization, Retention and Transparency

The guidelines' strict approach to data minimization and retention presents serious challenges for ensuring platform security and user safety. To prevent abuse, fraud, and attempts to circumvent enforcement systems, providers must be able to collect and retain sufficient data. Overly restrictive rules on minimization and retention risk undermining the integrity of platforms and weakening their ability to protect users.

The guidelines' restrictive interpretation of data minimization (para 14) is legally flawed and operationally unworkable for modern AI. It misrepresents the principle as an absolute mandate for *data avoidance* ("insofar as possible") rather than a proportionate test of *necessity* for a legitimate purpose. This position is not only technically unviable—large-scale datasets are a prerequisite for safe, effective, and unbiased AI models—but it also directly contradicts the more sophisticated guidance from other key authorities. The CNIL and EDPS have both clarified that data minimization is compatible with large-scale training, provided the focus is on proportionality and robust safeguards. We invite the EDPB to align its guidance with this established supervisory consensus to ensure consistency and legal certainty.

It is also important to clarify that the DSA itself contains extensive transparency obligations, including those related to content moderation, recommender systems, and advertising, which must be taken into account alongside the GDPR´s transparency requirements. Recognizing these overlapping obligations is crucial to avoid inconsistencies and ensure coherent and practical compliance.

3. Deceptive Design Patterns

At the outset, Bitkom notes that the EDPB's interpretation of Article 25 of the DSA may extend beyond the Board's traditional data protection remit, as this provision primarily addresses matters of non-personal data

The draft definition of "deceptive design patterns" is excessively broad and subjective. By capturing legitimate user experience (UX) and business practices under this heading, the guidelines risk creating legal uncertainty and stifling innovation. The conflation of persuasive design with manipulation disregards the need for a contextual, case-by-case assessment of actual user impact and intent. Furthermore, the guidelines' analysis of 'addictive behavior' (Para 47) designates common, legitimate features as inherently deceptive without providing any clear, objective evidence or scientific foundation for such complex claim**s**. It is worth noting that the European Commission has identified 'addictive behaviour' as an area that will require specific research and study before coming to any definitional finality in its work on the Digital Fairness Act. Without clearer and more objective criteria, companies face the risk of arbitrary enforcement and a chilling effect on innovation in digital services

4. Advertising Transparency and Profiling

The guidelines appear to treat the presentation of an advertisement to an individual as having legal effects on a data subject. This interpretation fundamentally misreads the law by conflating evaluative profiling with a final decision and by treating an "invitation" (an ad) as if it had the same "legal or similarly significant effect" as a credit refusal or employment decision. Furthermore, the guidelines' assumptions about processing 'vulnerability' data are operationally flawed, conflicting with data minimisation principles, pseudonymization, and the DSA's own prohibitions on such profiling. The guidelines appear to not recognise situations where even if a user engaged with content that might infer a special category, an online service provider does not, and has no intention of, using that to make inferences about that user. Basing this new guidance on the outdated 2018 WP29 ADM guidelines is a flawed foundation, as it fails to account for significant technological and market evolutions like the development of Privacy enhancing technologies (PETs).

Bitkom encourages the EDPB to revise its overly application of Article 22 GDPR and to clarify that this standard is reserved for decisions with profound, binding impacts—such as a credit refusal—and that the mere presentation of content or an advertisement does not meet this high threshold. Most personalised ads and algorithmic recommendations do not produce legal or similarly significant effects on individuals and should not be classified as automated decisions under Article 22 GDPR. 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 Guidelines should focus instead on high-risk cases, such as manipulative or discriminatory targeting, where intervention is justified.

Equally problematic is the attempt to equate all forms of targeted advertising with direct marketing. This interpretation is legally unsound, ignores established regulatory distinctions, and risks undermining legitimate and user-accepted forms of advertising that support the digital economy. To enhance practical applicability, it would be highly beneficial if the EDPB were to include concrete examples or case studies illustrating how these distinctions should be applied in practice.

5. Recommender Systems

The approach of the guidelines to recommender systems is particularly concerning. The attempt to apply Article 22 GDPR is a significant overreach that rests on flawed legal interpretations. First, the presumption that serving content creates a "legal or similarly significant effect" (para 84) is legally unfounded; it ignores the high standard established by the Article 29 Working Party, which reserved this for decisions with profound, lasting, or discriminatory impacts—a threshold that the mere presentation of content clearly fails to meet.

Second, the guidelines' definition of "profiling" is so expansive that it risks capturing basic, necessary functions like contextualization for language or region, which have no significant effect. This approach overlooks the practical benefits of such systems (para 81) and, if finalized, would disproportionately lower the Article 22 GDPR threshold in a

way that is both impractical and legally unsound. Besides, requiring profiling-based recommender systems to be used only after explicit user opt-in is fundamentally misaligned with how modern digital services operate. Personalisation is a core feature and user expectation that is essential for delivering relevant and engaging experiences. Treating personalisation as an exception, rather than the default, risks undermining service quality, competitiveness, and innovation, and ignores established user expectations and industry best practices. Regulatory approaches should recognize personalisation as a legitimate and foundational aspect of digital services, balancing privacy with the need for tailored experiences. Requiring VLOPs and VLOSEs to present profiling and non-profiling recommender system options equally and prohibiting the use of profiling recommender systems before selection by a recipient of the service significantly exceeds the requirements of the DSA.

Furthermore, requiring the equal presentation of profiling and non-profiling options is not explicitly required by the DSA or GDPR. It conflicts with legitimate product design and user experience optimization. Prohibiting all data collection for profiling while the non-profiling option is active is operationally rigid and technically unworkable, especially for essential functions like fraud prevention. This requirement would result in unnecessarily preventing VLOPs and VLOSEs from making legitimate user experience and design choices.

Bitkom recommends that the EDPB revise this guidance to ensure a balanced approach that respects the fundamental right to data protection (Art. 8, Charter) while also considering the freedom to conduct a business (Art. 16, Charter).

6. Protection of Minors

Bitkom supports strong protections for minors online. However, the guidelines' restrictive approach to age verification makes compliance operationally difficult. The EDPB's developing stance on robust age verification systems and the prohibition on the permanent storage of age data ignore the needs for differentiated protections (e.g., for younger versus older teens) and ongoing compliance obligations. It also prevents services from reacting to the evolving capacity of minors as they age up by offering age-appropriate experiences, if original age signals cannot be stored. Crucially, retaining a secure, pseudonymized age indicator avoids disruptive, repeated verification, thereby better supporting the principle of data minimisation. Repeated friction on age verification for a user also may potentially lead users to find ways to circumvent the repeated verification, or to seek out non-compliant service providers entirely.

Bitkom also encourages the EDPB to clarify that biometric processing used solely for age estimation—as distinct from unique identification—does not constitute special category data under Article 9. Additionally, the guidance could better reflect the flexible, intermediary 'age verification solutions' already in use within the EU. Providers should be able to rely on context-sensitive, proportionate measures that minimize data collection, such as confirmation mechanisms, unless higher-risk situations justify stronger safeguards.

7. Risk Assessment and Mitigation

The draft guidelines place excessive weight on privacy and data protection risks in the context of systemic risk assessments, thereby distorting the DSA's intended balance. Providers are expected to conduct continuous data protection impact assessments (DPIAs) and adapt them on an ongoing basis, without clear thresholds or guidance. This approach risks unnecessary duplication, creates disproportionate burdens, and undermines the effectiveness of risk assessments by diluting focus. The Guidelines may need to clarify when a DPIA is required in the context of the DSA's Article 34 risk assessments. DPIAs should only be required when specific processing operations present a high risk to individuals' rights and freedoms as explicitly required by the GDPR, rather than automatically following any DSA systemic risk finding. Clear delineation will avoid duplication, ensuring regulatory focus remains targeted and effective.

8. Codes of Conduct and Governance

The EDPB's insistence on the mandatory involvement of Data Protection Authorities (DPAs) and full alignment with GDPR obligations for all codes of conduct threatens to stifle industry-driven innovation and self-regulation. Furthermore, the absence of clear mechanisms for resolving overlaps between regulators creates significant legal uncertainty and the risk of double jeopardy. Cooperation between DSA and GDPR authorities is essential to avoid duplication and inconsistency, but each framework must retain its independent mandate. The DSA does not grant authorities parallel enforcement powers over GDPR obligations. Effective cooperation should occur through structured dialogue and consultation, especially with the lead data protection authority, ensuring coherence while respecting jurisdictional limits.

Conclusion

Ultimately, the **GDPR must remain the GDPR and the DSA must remain the DSA**. Each framework pursues distinct regulatory objectives and operates within its own legal logic. It is therefore essential that guidance on their interplay respects these boundaries and adheres to the definitions and concepts set forth in each respective instrument. Interpretative approaches should not result in the de facto extension of GDPR principles into areas governed by the DSA, but rather ensure coherent and balanced application in line with their respective legislative purposes

Bitkom represents more than 2,200 companies from the digital economy. They generate an annual turnover of 200 billion euros in Germany and employ more than 2 million people. Among the members are 1,000 small and medium-sized businesses, over 500 start-ups and almost all global players. These companies provide services in software, IT, telecommunications or the internet, produce hardware and consumer electronics, work in digital media, create content, operate platforms or are in other ways affiliated with the digital economy. 82 percent of the members' headquarters are in Germany, 8 percent in the rest of the EU and 7 percent in the US. 3 percent are from other regions of the world. Bitkom promotes and drives the digital transformation of the German economy and advocates for citizens to participate in and benefit from digitalisation. At the heart of Bitkom's concerns are ensuring a strong European digital policy and a fully integrated digital single market, as well as making Germany a key driver of digital change in Europe and the world.

Published by

Bitkom e.V.

Albrechtstr. 10 | 10117 Berlin

Contact person

Elena Kouremenou | Policy Officer for Data Protection

P +49 30 27576-425 | e.kouremenou@bitkom.org

Konstantin Peveling | Policy Officer for Media and Platforms

P +49 30 27576-321 | k.peveling@bitkom.org

Responsible Bitkom committee

WG Data Protection

WG Media Policy