DOT Europe response

EDPB Guidelines 3/2025 on the interplay between the DSA and the GDPR

Introduction

In Europe's evolving digital regulatory landscape, where multiple laws increasingly overlap, understanding the interplay between the Digital Services Act (DSA) and the General Data Protection Regulation (GDPR) is crucial. Only by clarifying this relationship can the protection of citizens' and consumers' data be ensured while they use online services. The DSA introduces a range of rules and obligations for intermediary service providers. Although the DSA is interpreted and enforced primarily by its own competent authorities, the European Board for Digital Services (EBDS) and the EU courts, several of its provisions directly intersect with the data protection framework. In particular, references to concepts such as "profiling" and "special categories of data" under the GDPR create significant implications for how intermediary service providers process personal data.

Therefore, the European Data Protection Board's (EDPB) draft Guidelines on the interplay between the DSA and the GDPR represent an important effort to clarify how two cornerstone pieces of EU legislation interact. However, the Guidelines, as currently framed, risk creating more uncertainty than clarity. To be effective, they would strongly benefit from a balanced and flexible approach that reflects operational realities and the full spectrum of DSA objectives. These insights could have been captured through earlier engagement with industry, in line with the EDPB's commitments under the Helsinki Statement. It is unfortunate that, despite this commitment to a more collaborative approach, the EDPB circulated the draft Guidelines in a near-final form rather than sharing preliminary reflections on some of the key principles underpinning them. Clear, objective, and proportionate requirements are needed, ones that safeguard data protection while also enabling innovation, ensuring user safety, and providing practical pathways for compliance. Additionally, DOT Europe is keen to understand to what extent the EDPB has engaged with the Digital Services Coordinators (DSCs) given the clear focus of the Guidelines on DSA. Broad institutional collaboration is very helpful to provide strengthened legal certainty and practical enforceability.

At present, the Guidelines systematically prioritise privacy and data protection above all other DSA objectives, neglecting the need for balance. By treating data protection as the overriding lens, they risk diminishing the DSA's role as a standalone legal instrument designed to foster a safe, transparent, and innovative digital environment. This narrow approach could lead to operational paralysis, legal uncertainty, and ultimately undermine the effective achievement of both data protection and broader digital policy goals.

The publication of these Guidelines coincides with the European Commission's upcoming Digital Simplification Package, which will examine the scope and potential overlaps of existing digital rules, and the review of the DSA under Article 91. In this context, it would be important for the EDPB to ensure that, should these Guidelines proceed to adoption, they are appropriately flagged for review in light of the outcomes of the digital simplification agenda.

Avenue Marnix 17, 1000
Brussels, Belgium
Tel: +32 (0) 472 26 83 02

WWW.DOTEUROPE.EU
Transparency Register: 53905947933-43

Moreover, the Guidelines blur the boundaries between enforcement under the DSA and the GDPR. Recent actions by certain national data protection authorities, such as the Berlin DPA[1], suggest an emerging trend of using DSA mechanisms to pursue GDPR enforcement. The EDPB should make clear that the DSA cannot serve as a shortcut for data protection enforcement and that the distinct purposes and procedures of each regulation must be respected. The Guidelines also make no mention of the GDPR's One-Stop-Shop (OSS) mechanism whereas it should remain central for cross-border privacy issues, even when DSA regulators are engaged.

The Guidelines are also incomplete, as they do not address several DSA provisions that entail personal data processing and data sharing with third parties. In particular, there is no guidance on the data sharing arrangements with out-of-court dispute settlement bodies required under Article 21 DSA.

With this paper, DOT Europe sets out its perspective on the Guidelines. The document is structured into two main sections: the positive elements of the Guidelines, and the key concerns they raise. We hope these elements will be helpful to achieve Guidelines that enhance legal certainty for companies while strengthening safety for European citizens.

Positive elements of the draft Guidelines

The draft EDPB Guidelines include several elements that can be viewed positively, reflecting a constructive approach to the interplay between the GDPR and the DSA. These aspects demonstrate an effort to provide clarity, reinforce fundamental principles, and set a framework for proportionate and coherent application of both legal instruments. In this section, we highlight the main positive points identified by DOT Europe.

- **Paragraph 9** and **paragraph 118** clarify that, as provided by case law of the Court of Justice of the European Union (CJEU), where two legal acts of the same hierarchical value, such as the DSA and the GDPR, "do not establish priority of one over the other, they should be applied in a compatible manner, which enables a coherent application of them." Thus, although neither the GDPR nor the DSA provides specific rules for cooperation between competent authorities under the DSA and data protection supervisory authorities, in light of Article 8(3) of the Charter and the principle of sincere cooperation under Article 4(3) TEU as interpreted by the CJEU, they should consult and cooperate sincerely with each other in order to assess whether both the DSA and the GDPR are respected. We consider this a very important statement. However, we note that the procedural basis of these Guidelines lacks transparency, in the sense that it is unclear whether and to what extent the EDPB has engaged in substantive consultation with the EBDS and the DSCs. We consider this omission significant, especially because the EDPB largely advocates for greater inter-regulatory cooperation. Finally, Joint Guidelines between the EDPB and EBDS would have benefited from a higher degree of cooperation and legal certainty.
- **Paragraph 17** and **paragraph 18** recognise that the most appropriate legal basis under the GDPR, in cases where intermediary service providers carry out processing in the context of their voluntary, own-initiative investigations or other measures to detect, identify, and remove (or disable access to) illegal content (Article 7 DSA), would be Article 6(1)(f) ('legitimate interests'). Furthermore, para. 18 states that the first of the three cumulative

[1] See here: https://www.reuters.com/sustainability/boards-policy-regulation/deepseek-faces-expulsion-app-stores-germany-2025-06-27/

conditions to justify the "legitimate interest" (the interest pursued must be legitimate) is clear when it comes to detecting and addressing illegal content in intermediary services to protect the recipients of the service, "in particular where such content can be disseminated to the public via an online platform." The Guidelines implicitly treat any inaccurate or imperfect detection as potentially problematic, as the controller must justify both necessity and proportionality very strictly. We consider this too strict, as even minor mistakes could be used to argue that processing violates the legitimate interest criteria.

- **Paragraph 92** reaffirms that any processing of personal data for purposes such as age assurance must be proportionate to the objectives pursued. While the Guidelines adopt a relatively narrow interpretation of proportionality, requiring that no less intrusive means be available to mitigate risks, this emphasis on privacy can be welcomed. In particular, raising the privacy standard for age verification may help prevent the premature introduction of overly extensive or intrusive EU-wide age verification requirements, even if it presents some tension with broader harmonization goals (see the section below).

Key concerns

As a first general remark, we underline that these EDPB Guidelines are meant to explain how GDPR applies where DSA obligations require or imply processing of personal data, therefore, they should not be used to offer interpretation of the DSA itself. The EDPB does not have a legal mandate to interpret the DSA in the same way that the European Commission or the DSCs do. Thus, **paragraphs 52, 67, 75-78, 86, 87** and **section 2.7** should be reviewed to ensure that the EDPB does not exceed its mandate.

Automation and content moderation

- The DSA acknowledges the value of automated means in the context of content moderation and requires online intermediaries to be transparent on their use towards users. Automated means, with safeguards, are particularly useful when providers operate at a large scale.
- The Guidelines unfortunately adopt a sceptic approach in the context of voluntary own-initiative investigations and compliance with legal requirements, enabled under Article 7 DSA.
- **Paragraph 15** states that technologies for voluntary detection and tackling of illegal content potentially entail risks as they tend to have high error rates. We point out that this is a point-in-time assessment and technologies will evolve. We suggest to reframe this risk as a factor influencing the legitimate interest three-step test rather than as a fact.
- Furthermore, **paragraph 22** considers that some actions based on automated processing of data taken by providers under Article 7 DSA may fall under Article 22(1) GDPR, which prohibits such decisions when they have legal effects on the user or similarly significant effects. However, the Guidelines fail to explain why measures taken by providers following Article 7 DSA would qualify as Article 22(1) practices, particularly to what extent they could have legal or similar effects on users. It should be noted that the Article 29 Working Party clarified that this provision is intended to cover only "serious impactful effects," with examples such as refusal of a credit application and denial of citizenship[2].
- We recall that most content moderation decisions primarily enforce providers' terms and conditions, which the user has consented to by using the service. We argue that most

[2] See Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, adopted on 3 October 2017 and last revised and adopted on 6 February 2018, p.21

proactive moderation decisions do not have the kind of legal or significant effects contemplated by the GDPR in its provisions on automated decision-making. For most types of content these voluntary own-initiative investigations and any personal data processed will not meet the threshold for automated decision-making (ADM) as content will be of an innocuous nature, and personal data processing will be only a limited part of these investigations. Pending the justification that measures meet the threshold of Article 22(1) GDPR, we consider that the Guidelines offer an excessive and disproportionate recommendation, creating significant operational burdens and disregarding DSA's objectives. The Guidelines reference data minimisation in relation to notice and action systems, however the Guidelines should also consider other data protection principles like accuracy and purpose limitation and take into account that these are given equal importance under the GDPR.

- We agree with the Guidelines that notice and action mechanisms must protect users' personal data (see **paragraph 30**) while ensuring that providers can effectively respond to reports of illegal content. However, it should be noted that providers also need flexibility to verify notifier identities, where reasonably necessary, to prevent abuse or assess legality.

Deceptive Design Patterns

- **Section 2.3** goes beyond the EDPB's mandate, which, as per Article 25(2) DSA, is limited to deceptive design patterns identified in the GDPR. In other words, Article 25(1) covers only dark patterns concerning the processing of non-personal data. This is acknowledged in **paragraphs 43 and 44**.
- **Paragraphs 46 and 47** are, on the contrary, particularly problematic in that regard. The EDPB incorrectly conflates deceptive design patterns with design features that "may cause addictive behaviour" or "may stimulate behavioural addictions of recipients of the service" in Recitals 81 and 83 DSA whereas the concepts are not linked in the DSA itself. Moreover, Recitals 81 and 83 DSA relate to systemic risk assessment under Article 34 DSA and not to Article 25 on deceptive design practices (Recital 67 is the corresponding recital). Features identified as possibly leading to "addictive behaviour" in DSA risk assessments do not automatically qualify as dark patterns. In particular, the items enumerated in the Guidelines cannot be assumed to be inherently "deceptive," and the EDPB has not offered sufficient evidence or legal justification for such an assertion, despite its potentially wide-reaching consequences.
- Moreover, references to "addictive behaviour" as a possible source of systemic risks are clearly outside of the EDPB's remit and expertise. In their current state, these paragraphs in the Guidelines venture into generalities and this risks capturing legitimate design practices which enhance user experience. We are concerned by this approach as it could lead to arbitrary enforcement and increase legal uncertainty.
- Moreover, if the ambiguity regarding the supervision of dark patterns persists, this could result in regulation of this issue by multiple authorities, which will create confusion and legal uncertainty. To avoid a disjointed, complex, duplicative and inefficient regime regulating design that might cause 'addictive behaviour', we strongly urge the EDPB to consider its position on design that "may cause addictive behaviour", and the interplay with deceptive design practices more broadly, and consult and coordinate with the appropriate bodies.
- Finally, **footnotes 77, 78, and 79** refer to a resolution of the European Parliament in order to back its claims. However, this document has no legal value and should instead be considered as a political declaration.

- For the reasons listed above, we encourage the EDPB to revise and clarify these sections, explicitly confirming that the examples provided apply only in cases involving the processing of personal data, and are therefore subject to the GDPR rather than Article 25(1) DSA, in line with Article 25(2) DSA.

Transparency requirements in relation to advertising

- **Paragraph 52** recognises a tension between Article 26 DSA and GDPR requirements. Indeed, while DSA requires transparency to the user after data processing, GDPR requires transparency to the user at the time of data collection and before data processing. We regret that the Guidelines do not offer solutions to reconcile these obligations, especially as this could avoid fragmented implementation and user confusion.
- **Paragraph 62** mentions that presenting advertising online could have legal or significant effects on users, which we question. The guidelines appear to blur the distinction between the analytic phase of profiling and the final decision that produces legal or similarly significant effects. We also highlight that advertising does not generate legal or financial consequences for users in the way decisions about credit or employment can. The guidance also appears to assume that providers handle "vulnerability" data, which is inconsistent with data minimisation and the DSA's own restrictions. Therefore, we encourage the EDPB to base its guidance on demonstrable impact on users rather than on the nature of the profiling. The Guidelines should also clarify that the selection and presentation of advertising does not constitute ADM falling under Article 22(1) GDPR.
- **Paragraph 76** adopts a particularly restrictive reading of the Article 26(3) DSA prohibition on serving ads based on profiling using special categories of personal data. According to the Guidelines, even if a provider can rely on an appropriate legal basis under Article 6(1) GDPR and an appropriate derogation under Article 9(2) GDPR, the DSA bans such profiling. However, we call for a balanced interpretation in this case, particularly in view of Recital 69 DSA, which states that "This prohibition is without prejudice to the obligations applicable to providers of online platforms or any other service provider or advertiser involved in the dissemination of the advertisements under Union law on protection of personal data."
- In addition, Example 2 in the Guidelines appears to take the position that a user has visited a place of worship or purchased e.g. kosher foods, is in itself an "inferred religious belief". This is an excessively broad interpretation of special category data and could prevent the industry at large from using any signals from any sensitive videos or where interests could relate to sensitive topics, even if those signals are not used to create special category data inferences or were not derived from sensitive categories of data. The Guidelines should clarify that an inference must be created or special category attributes must be attributed to a user which is then used to display an ad in order to consider that special category data has been processed.

Recommender Systems

- We disagree with the interpretation in **paragraph 83** that recommender systems using personal data always entail risks to individuals. This is not always the case and overlooks significant user benefits of recommender systems. We recommend a more nuanced approach that acknowledges such systems *may* entail risks, rather than presenting this as a blanket statement, as reflected in Recital 70 DSA.
- We disagree with the interpretation found in **paragraph 84** that recommender systems qualify as "decisions" under Article 22(1) GDPR. The Article 29 Working Party made clear that Article

22(1) is triggered only where a decision has substantial, lasting effects on a person's circumstances or opportunities. Showing content that a user can freely ignore clearly falls below this threshold. This paragraph adopts a speculative tone which is not helpful in the context of Guidelines. Moreover, the definition of "significant effect on users" found in **footnote 103** is not applied in the context of recommender systems, which could have been useful to substantiate the EDPB's claims.

- In addition to the above and to provide a more complete picture, we suggest expanding the context in **paragraph 84** to include that the referenced guidance (see **footnote 103**) also contains a valuable counter-example that clarifies when targeted advertising is not considered to have a significant effect. Including this would offer a more balanced and comprehensive view.
- **Paragraph 85** seems to expand the scope of Article 22(1) GDPR by considering that recommendations and proposals amount to decisions. We disagree with this interpretation for reasons outlined above. Moreover, the Guidelines refer to the Advocate-General opinion on the case C-634/21 OQ v SCHUFA, which relates to a decision based on automated scoring of a data subject in the banking context. This is fundamentally different from recommending content on online platforms.
- As mentioned above, **paragraph 87** goes beyond the DSA and the EDPB's remit as it mandates an "equal presentation" for profiling and non-profiling options. This is also in conflict with the clear wording of Articles 27(3) and 38 of the DSA and paragraph 86 of the Guidelines. These provisions stipulate that VLOPs must offer at least one option of their recommender systems that is not based on profiling, and that recipients of the service must be able to select and modify their preferred option at any time through a functionality that is directly and easily accessible from the relevant section of the platform's interface. However, the DSA does not require VLOPs to present both options simultaneously, to default to the non-profiling option, or to obtain users' opt-in before providing a personalised recommender system. Rather, it simply obliges platforms to ensure that a non-profiling alternative exists and remains easily accessible.
- Even when users choose not to view recommendations based on profiling, the DSA does not restrict or prohibit the processing of personal data for profiling purposes, provided that such processing is carried out lawfully and in compliance with data protection rules. Moreover, this conflicts with legitimate product design and user experience considerations. In line with **paragraph 5** of the Guidelines, the EDPB should refrain from interpreting the DSA, as this is for competent authorities under the DSA and EU courts to do so.
- We would also question the recommendation in **paragraph 88** not to retain a history of choices made by users when it comes to the modification of their recommender system parameters, i.e. user choice history. This interpretation appears to lack a clear legal basis and its rigid application would reveal counterproductive both for users and online platform providers (in the context of e.g., fraud prevention and GDPR accountability to manage user consent and ensure settings are applied consistently) provided this is done lawfully and in compliance with data protection rules. This is why we encourage the EDPB to review this paragraph also in light of Section 6.5.2 (point 67.c in particular) of the Guidelines on measures to ensure a high level of privacy, safety and security for minors online, pursuant to Article 28(4) of Regulation (EU) 2022/2065 (hereafter, "Article 28 Guidelines").

- More generally, treating personalisation as an exception rather than the default risks undermining service quality, competitiveness, and innovation, while disregarding established user practices and industry standards.

Protection of Minors

- DOT Europe is intrigued by the EDPB's proposed approach to age assurance in **section 2.6**. It seems particularly restrictive and inconsistent with other EU rules and initiatives pertaining to minor protection online.
- First, **paragraphs 92 and 93** indicate that "mechanisms that enable unambiguous online identification" should be avoided. However, Article 28 Guidelines consider the use of age verification to be proportionate in some cases to provide a high level of privacy, safety and security for minors on online platforms. Moreover, the Commission itself pointed to an EU age verification app anchored to the EU Digital Identity Wallet, which is based on government-issued identity credentials, as meeting the standards of the Article 28 Guidelines. The difference between the guidance provided by Article 28 Guidelines and these EDPB Guidelines puts online platform providers in an impossible situation.
- **Paragraph 94** prohibits the permanent storing of age or age range data after age assurance of a user has been carried out. This could reveal problematic to provide age-appropriate experiences to certain users, e.g., minors, and take into account their developmental stages. Furthermore, Article 28 Guidelines enable online platform providers to store the user's age group after age has been verified (see paragraph 39). This approach would be highly impractical for platforms offering distinct age-based experiences within minors' age ranges. Requiring repeated re-verification/estimating as users mature would not only disrupt the user experience but could also result in unnecessary and excessive data processing, undermining the principle of data minimisation. Such restrictions may also limit providers' ability to discharge their ongoing and continuous obligations under Article 28(1) DSA.

Risk assessment and mitigation

- We recall that the DSA strikes a balance between different risks and how VLOPSEs are to mitigate them. While we appreciate the general focus of the EDPB on privacy and data protection risks, this should not come at the expense of others. In that sense, **paragraphs 99 and 107**'s expectation to continuously carry out data protection impact assessments (DPIAs) in systemic risks assessments seem superfluous and particularly burdensome, especially considering heavy requirements already falling on VLOPSEs as part of the regular reporting and transparency requirements. We are concerned that such a requirement would lead to unnecessary duplication of efforts in an already demanding reporting schedule. In our view, a DPIA 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.
- **Paragraphs 117 and 118** acknowledge that there is no explicit duty of cooperation in the DSA and GDPR. However, it is regrettable that the Guidelines do not suggest a way forward. Risks of legal uncertainty and *ne bis in idem* cases are particularly high therefore the Guidelines should insist on the need for DPAs and competent authorities under the DSA to establish cooperation mechanism. This would also avoid any circumvention of the GDPR procedures by authorities seeking to enforce the GDPR using DSA mechanisms.

- Similarly, the absence of clear cooperation mechanisms to resolve regulatory overlap could reveal problematic, also in the case of DSA Codes of Conduct (see **section 2.8**). Therefore, we would value *ex-post* EDPB opinions on potential Codes negotiated under the DSA, when relevant to the GDPR.
- Finally, we welcome the reference to Article 8(3) of the Charter and the principle of sincere cooperation under Article 4(3) TEU as interpreted by the CJEU (**paragraph 113).** However, the Guidelines do not specify the timing of consultations. It would be useful to clarify that consultations should occur at a meaningful time before decisions are issued and for guidance development where frameworks overlap.

Counting Monthly Active Recipients

- The Guidelines do not address the obligation to count monthly active recipients (MARs) under Article 24(2) DSA, nor the significant interplay, and tension, with the GDPR and ePrivacy Directive. Under the DSA, online platforms must publish information on average MARs in the EU, avoid double-counting where possible, and may exclude inauthentic users (e.g. bots) if technically feasible. However, a recent CJEU ruling[3] clarifies that overcounting is preferable to undercounting from a DSA compliance perspective. This includes counting users who did not consent to cookies and non-logged-in users, to avoid underreporting. We therefore urge the EDPB to address this legal tension in its Guidelines and provide clarity on how platforms can comply with the DSA's MARs reporting requirements without breaching data protection and ePrivacy rules.

Conclusion

Overall, while the EDPB Guidelines make important efforts to clarify the interaction between the GDPR and the DSA, they leave significant gaps and raise numerous practical and legal concerns. DOT Europe welcomes certain positive elements, such as the recognition of coherent application of EU law, the acknowledgment of legitimate interests for voluntary detection, and the emphasis on proportionality in age assurance. However, the Guidelines often prioritise data protection above all other DSA objectives, adopt overly strict interpretations of key provisions, and risk creating operational burdens, legal uncertainty, and regulatory overlap.

To be effective, the Guidelines should adopt a balanced, risk-based approach that reflects operational realities, ensures proportionate compliance requirements, and provides practical solutions for harmonising the DSA and GDPR. Clear distinctions between the enforcement competencies of DSA and GDPR authorities must be maintained, and any legal basis for processing personal data under the DSA should be demonstrably necessary and proportionate to achieve the objectives set out in the relevant DSA provisions. Addressing these points would enhance legal certainty, preserve innovation, and strengthen the safe, efficient functioning of online services in Europe.

[3] Court of Justice of the European Union, 3 September 2025, Zalando SE / Bundesverband E-Commerce und Versandhandel Deutschland eV, ECLI:EU:T:2025:821