Commentary Guidelines 3/2025 on the Interplay between the DSA and the GDPR

Artigo 80 – Associação Portuguesa para a Defesa do Titular de Dados Pessoais, is a national non-profit association established under Portuguese law, dedicated to the defence and promotion of the fundamental rights of data subjects. The association acts as a civic interlocutor with public and private entities, with a particular focus on GDPR compliance, the promotion of digital literacy, and the strengthening of citizens' trust in the European digital environment.

In the context of the public consultation on Guidelines 3/2025, Artigo 80 welcomes the EDPB's efforts to clarify the interaction between the Digital Services Act (DSA) and the GDPR. Nevertheless, we identify several gaps and practical challenges in the protection of data subjects' rights and submit recommendations for stronger safeguards. The GDPR should remain the minimum level of protection that cannot be undermined by the implementation of the DSA.[1]

1. Identified gaps and challenges

1.1 Automated content removal (Art. 7 DSA)

Article 7 permits voluntary investigations, including the use of automated tools. However, without harmonised safeguards, there is a significant risk that automated systems — particularly those relying on machine learning — may generate false positives, leading to the unjustified removal of lawful content and restrictions on freedom of expression and information (Article 11 CFREU). Where such decisions have a significant effect on users, they fall within the scope of Article 22 GDPR and require meaningful human oversight and procedural safeguards.

1.2 Notice and action mechanisms (Arts. 16–17 DSA)

The DSA requires notifiers to provide sufficient information to identify allegedly illegal content. However, disclosure of notifier identities may expose individuals to retaliation, thereby discouraging legitimate reporting. Without clear limits on the collection and disclosure of notifier data, there is a risk of infringing the GDPR principles of data minimisation (Art. 5(1)(c)) and accuracy (Art. 5(1)(d)).

1.3 Complaints and account suspension (Arts. 20–23 DSA)

The DSA establishes complaint-handling mechanisms and access to independent out-of-court dispute settlement bodies. While positive, these provisions lack sufficient guarantees to ensure timely and effective redress. Decisions on suspensions or restrictions may also be based on inaccurate data, contrary to Article 5(1)(d) GDPR.

[1] This approach reflects the status of the GDPR as the horizontal framework for data protection in the EU. It sets a non-derogable minimum standard of protection for data subjects' rights, which sector-specific instruments such as the DSA may complement or strengthen, but never weaken. See Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L119/1, arts 1(2) and 8 CFREU.

geral@artigo80.pt
https://artigo80.pt
Associação Portuguesa Para A Defesa Do Titular De Dados Pessoais.
Avenida Calouste Gulbenkian, nº 1811, Loja 7, 4460-403 Senhora da Hora
Portugal - NIPC 516 964 119

1.4 Advertising and profiling (Art. 26 DSA)

Although Article 26 prohibits the use of special categories of data for targeted advertising, transparency obligations alone may not guarantee genuine understanding by users. Excessive or highly technical disclosures risk creating consent fatigue (a concern repeatedly acknowledged by data protection authorities), leaving users vulnerable to manipulative practices or to discriminatory targeting, which is inconsistent with the GDPR principles of fairness and purpose limitation, and with the prohibition of discrimination under Article 21 CFREU.

1.5 Recommender systems (Arts. 27 and 38 DSA)

The obligation to provide a non-profiling option is welcome. However, the DSA does not require independent verification that such options are effective. In some contexts, recommender systems may constitute automated decision-making with significant effects under Article 22 GDPR, thereby requiring additional safeguards.

1.6 Protection of minors (Art. 28 DSA)

Article 28 prohibits profiling-based advertising directed at minors, representing a strong substantive safeguard. Yet uncertainty remains regarding privacy-preserving methods for age verification. Reliance on official documents or biometric checks risks exposing minors to unnecessary privacy intrusions. Harmonised standards are needed to ensure proportionate and privacy-preserving solutions consistent with the GDPR and children's rights.

1.7 Systemic risk assessments (Arts. 34–35 DSA)

While the DSA requires systemic risk assessments, these obligations are not integrated with Data Protection Impact Assessments (DPIAs) under Article 35 GDPR. The resulting fragmentation risks duplicating efforts and undermining accountability. A more holistic, integrated framework would ensure consistency and effectiveness.

2. Recommendations for stronger mechanisms

2.1 Human oversight and effective redress

Any decision with a significant impact on fundamental rights — including removal of content, account suspension, or exclusion from advertising — must be subject to effective and documented human review,[2] coupled with access to impartial and timely remedies.[3]

[2] The CJEU has consistently underlined the need for effective safeguards and independent oversight where automated or large-scale data processing affects rights, most notably in Joined Cases C-293/12 and C-594/12 Digital Rights Ireland [2014] ECLI:EU:C:2014:238. Similarly, the ECtHR has stressed the importance of procedural safeguards in automated decisions affecting rights in López Ribalda and Others v Spain (2019) 68 EHRR 7.

[3] The CJEU has highlighted that effective judicial protection is a general principle of EU law, requiring timely remedies: Case C-73/16 Puškár v Finančné riaditeľstvo Slovenskej republiky [2017] ECLI:EU:C:2017:725. Delays or lack of redress undermine the very essence of the right to an effective remedy under Article 47 of the Charter of Fundamental Rights of the EU (CFREU).

2.2 Protected anonymity for notifiers

The identity of notifiers should only be disclosed under judicial order or when strictly necessary and proportionate, with prior notice to the notifier. This safeguard would protect individuals from retaliation and ensure that legitimate reporting is not discouraged.[4]

2.3 Advertising safeguards and transparency

Platforms should provide plain-language explanations of profiling techniques, the categories of data used, and their likely impact on user choice. In addition, substantive restrictions should prevent discriminatory or manipulative profiling practices.[5]

2.4 Verification of recommender systems

Recommender systems should undergo periodic independent assessments to verify that non-profiling options are effective and that covert data collection does not occur.[6]

2.5 Privacy-preserving age assurance

Age verification methods should rely on privacy-preserving technologies such as zero-knowledge proofs or contextual checks. The permanent storage of identity documents or age data should be explicitly prohibited to avoid unnecessary risks to children's privacy.[7]

2.6 Integrated GDPR–DSA risk framework

A single, integrated reporting model should be developed to cover both GDPR and DSA obligations. This model should include mandatory metrics on the impact on fundamental rights, ensuring a coherent and efficient regulatory approach.[8]

---

[4] The ECtHR has protected anonymity as part of freedom of expression under Article 10 ECHR, emphasising the chilling effect of compelled disclosure, e.g. Goodwin v United Kingdom (1996) 22 EHRR 123. This principle is equally applicable to notifiers whose safety and willingness to report depend on the assurance of confidentiality.

[5] The CJEU has emphasised the importance of clear and precise information in the context of data processing in Case C-136/17 GC v CNIL [2019] ECLI:EU:C:2019:773. The ECtHR has equally highlighted that lack of safeguards against discriminatory or manipulative use of personal data may undermine fundamental rights, see Big Brother Watch and Others v United Kingdom (2021) 72 EHRR 17.

[6] In Case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems (Schrems II) [2020] ECLI:EU:C:2020:559, the CJEU underscored the necessity of effective oversight and enforceable accountability mechanisms in contexts involving large-scale data processing. Independent audits of recommender systems operationalise these principles in the algorithmic environment.

[7] The ECtHR has made clear that children are entitled to special protection in the digital environment, see K.U. v Finland (2009) 48 EHRR 52, where the Court highlighted States' positive obligations to safeguard minors' privacy. Privacy-preserving methods ensure compliance with both child protection and proportionality under Article 8 ECHR.

[8] In Case C-362/14 Schrems v Data Protection Commissioner (Schrems I) [2015] ECLI:EU:C:2015:650, the CJEU emphasised the need for a comprehensive assessment of the level of protection of fundamental rights, taking into account both legal and practical safeguards. This reasoning supports the call for integrated GDPR–DSA risk assessments, avoiding fragmented reporting and ensuring consistency.

3. Conclusion

Artigo 80 commends the EDPB for its efforts to clarify the interplay between the GDPR and the DSA. Nonetheless, without reinforced safeguards, there is a tangible risk that the Guidelines may result in predominantly formal compliance rather than in the **effective and practical protection of data subjects' rights**.

We therefore urge the reinforcement in the following key areas: **robust human oversight of automated decisions, protection of notifier anonymity, accessible, harmonised and effective redress mechanisms, stronger safeguards in profiling and advertising, independent verification of recommender systems, privacy-preserving age assurance methods, and the integration of GDPR and DSA risk assessment frameworks**.

By embedding these safeguards, the Guidelines can achieve a coherent and high standard of fundamental rights protection across the Union, thereby fostering user trust, strengthening accountability, and ensuring that the European digital environment remains safe, fair and rights-compliant, in full respect of the principle of proportionality and the primacy of the GDPR as the baseline of fundamental rights protection.

We respectfully submit these observations for your consideration and stand ready to contribute further to the refinement of the Guidelines.

Senhora da Hora, 21 September 2025

Virgilio Lobato Cervantes

President, Artigo 80

geral@artigo80.pt

https://artigo80.pt

Associação Portuguesa Para A Defesa Do Titular De Dados Pessoais.
Avenida Calouste Gulbenkian, nº 1811, Loja 7, 4460-403 Senhora da Hora
Portugal - NIPC 516 964 119