Anitec-Assinform

GUIDELINES 3/2025 ON THE INTERPLAY BETWEEN THE DSA AND THE GDPR RESPONSE TO THE PUBLIC CONSULTATION

Sommario

Associazione Italiana per l'Information and Communication Technology (ICT)
Milano, Via San Maurilio 21, 20123
Telefono 02 0063281
segreteria@anitec-assinform.it – anitec-assinform@pec.it – www.anitec-assinform.it
P.IVA: 10053550967 C.F.: 10053550967

Anitec-Assinform

1. INTRODUCTION

Anitec-Assinform is the business association representing the Information and Communication Technology industry in Italy. As such, we present the unique perspective of the Italian digital ecosystem, comprised of major global players, national champions and several fast-growing SMEs.

We welcome the EDPB's work to ensure coherent interpretation and application of the DSA and the GDPR and we are grateful to be given the opportunity to respond to the consultation.

However, we regret that the guidelines have not been produced in cooperation with Digital services coordinators (DSC) and the European Board for Digital Services (EBDS). Not only creating legal uncertainty by omitting the reading of the main enforcers of the DSA, it contradicts the EDPB's recent Helsinki Statement to promote a cross-regulatory landscape. To ensure a consistent and balanced interpretation, we urge the EDPB to formally consult the EBDS before finalizing this guidance.

The Guidelines offer valuable clarity in several key areas, however, we believe there are a number of areas of concern with the interpretation set out by the Guidelines, as well as areas where the Guidelines would benefit from greater clarity.

This document aims to address the main issues that the Guidelines may cause keeping in mind that a risk-based, proportionate approach should remain the guiding principle.

2. PROPORTIONALITY AND RISK-BASED APPROACH

The principle of proportionality must remain at the heart of the interplay between the Digital Services Act (DSA) and the General Data Protection Regulation (GDPR). Both frameworks pursue important and complementary objectives — ensuring a safe, transparent digital environment while safeguarding individuals' fundamental rights, including privacy. However, effective implementation requires a balanced and risk-based approach that recognises the diversity of online services, operational realities, and varying levels of risk to users.

The EDPB's interpretation should avoid imposing uniform, one-size-fits-all obligations that disregard context or scale. Data protection and online safety

measures should be commensurate with the nature, scope, context and purpose of processing as required by Article 5(1)(a) and Recital 76 GDPR. In practice, this means that higher-risk activities — such as manipulative targeting, discriminatory advertising, or profiling likely to produce significant effects — warrant stronger safeguards, whereas routine, low-impact operations (e.g. standard content moderation, presentation of an advertisement or recommender systems) should be treated proportionately.

A genuinely risk-based framework also ensures the necessary balance between privacy protection and other fundamental rights, including freedom of expression, access to information, and the freedom to conduct a business, as affirmed by Recital 4 GDPR and consistent CJEU case law. Maximising data protection in every instance without considering these parallel rights would produce disproportionate and counterproductive outcomes — for example, hampering the ability of platforms to detect and remove illegal content or to provide age-appropriate experiences for minors.

Proportionality further implies that compliance obligations must remain technically and operationally feasible, especially for small and medium-sized enterprises. A balanced, scalable approach allows all actors — regardless of size — to uphold high standards of user protection without undermining competitiveness.

In sum, the EDPB's final Guidelines should explicitly reaffirm that both the GDPR and the DSA are "risk-based instruments", designed to adapt regulatory effort to the level of potential harm. Proportionality should guide every interpretative choice, ensuring that data protection obligations support — rather than impede — the achievement of a safer, more innovative, and rights-respecting digital environment in the EU.

3. COORDINATED BUT DISTINCT REGULATORY OVERSIGHT

Effective cooperation between DSA and GDPR authorities is crucial to prevent duplication and inconsistency, while ensuring that each framework maintains its own mandate. The DSA does not grant parallel enforcement powers over GDPR obligations, so coordination should take place through structured dialogue and consultation, particularly with the lead data protection authority.

However, the draft EDPB Guidelines fail to establish clear and predictable rules for such cooperation, creating legal uncertainty that threatens the functioning of the

Digital Single Market. The absence of formal consistency mechanisms risks duplicative investigations and conflicting enforcement by Data Protection Authorities (DPAs) and Digital Services Coordinators (DSCs), potentially violating the principle of *ne bis in idem*. This improper conflation of competencies has already been observed with a DPA leveraging DSA framework to pursue matters that fall under the GDPR's remit.

This ambiguity could result in overlapping competencies and regulatory paralysis, with platforms facing contradictory rulings under the two regimes. Clear delineation of responsibilities and formal cooperation mechanisms are therefore essential to ensure coherence, efficiency, and legal certainty. The Guidelines must also explicitly preclude the use of the DSA as a proxy for data protection enforcement and, separately, reaffirm the primacy of the One-Stop-Shop mechanism for all cross-border data protection supervision.

4. NOTICE AND TAKE DOWN SYSTEMS (ARTICLE 17)

The guidelines state that when implementing the "notice and action" system under the DSA, it is essential to ensure strong safeguards for the protection of personal data of all parties involved, including the notifier. Personal data should be limited to what is strictly necessary for the purposes defined in the DSA. Providers, in particular, should not request additional personal information beyond what is specified in Article 16(2), unless expressly required by the Regulation. This interpretation is problematic; Article 16(2) is not an exhaustive list, and providers must be able to request the information necessary to meet the DSA's requirement for a 'sufficiently precise and adequately substantiated' notice.

We believe that 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.

Inaccurate or incomplete data interferes with the proper operation of the notice and action mechanism and could lead to wrongful accusations being made and incorrect action being taken.We would welcome confirmation that 'legal obligation' (Article 6(1)(c)) is the appropriate legal basis for processing data related to these notices, similar to the confirmation in Paragraph 20 regarding data subject rights.

Similarly, the claim that notifier identification should be optional contradicts Recital 53 of the DSA, which explicitly encourages asking for identity to avoid misuse. Anonymous reporting. should not be suggested as the default approach for notice and action mechanisms. Providers also need flexibility to verify notifier identities where reasonably necessary to prevent abuse or assess legality. The DSA make clear that, although anonymous reporting must be allowed in certain limited cases, it generally requires identification of the notifier.

The Guidelines should emphasize enabling privacy-preserving safeguards that still allow responsible handling of abuse and illegal content.

5. AUTOMATED DECISION MAKING (ARTICLE 22)

We believe the draft Guidelines should make clear that voluntary investigations and proactive moderation efforts by platforms to detect and remove illegal or harmful content are unlikely to constitute automated decision-making (ADM) under Article 22(1) of the GDPR. Most proactive moderation activities do not produce the kind of legal or similarly significant effects contemplated by Article 22, its accompanying recitals, or the Article 29 Working Party Guidelines on ADM.

The proposed Guidelines, however, risk expanding the scope of core GDPR principles, particularly Article 22(1)—beyond their intended meaning, in a way that could seriously impair the fundamental functioning of online services. The EDPB suggests that routine, large-scale operational activities, such as automated content removals, recommender systems, or presentation of an advertisement, could qualify as decisions producing "legal or similarly significant effects." This interpretation overlooks the high threshold explicitly required by Article 22 (1), which the Article 29 Working Party clarified applies only to decisions with "serious impactful effects," such as the refusal of credit, denial of citizenship, or other actions affecting an individual's legal rights.

This approach reflects a misunderstanding of the scale and nature of online safety operations. Content moderation is an industrial-scale process, essential to achieving the DSA's core objective of maintaining a safe online environment. The impact of any single moderation decision is typically minor and cannot reasonably be equated with a major life event or a significant interference with individual rights.

Most personalized advertising would also not have such impacts on individuals. Thus, the Guidelines should also clarify that targeted advertising will only be considered ADM under Article 22(1) of the GDPR where the effect of a decision is a legal effect or similar to a legal effect. This is in line with the Article 29 Working Party Guidelines on ADM.

If every automated content removal were to trigger the procedural requirements of Article 22—such as the right to human intervention— the operational friction would become unmanageable. Platforms would be forced to choose between attempting the impossible task of manual review for all content or scaling back automated detection systems altogether. The likely outcome would be a drastic reduction in the ability to identify and remove illegal or harmful content, undermining the DSA's objectives and making the internet less safe for users.

Accordingly, the Guidelines should reaffirm that voluntary, own-initiative investigations and associated personal data processing generally do not meet the ADM threshold under Article 22, as the content in question is often innocuous and any personal data processing represents only a limited part of these activities.

6. DARK PATTERNS - DECEPTIVE DESIGN (ARTICLE 25)

The examples provided in relation to dark patterns suggest that design features such as infinite scroll, autoplay or continuous streaming, and other common, legitimate features could be considered inherently deceptive. This approach is problematic as it designates these features as harmful without the necessary contextual, case-by-case assessment of their design, user intent, and actual impact. The Guidelines appear to treat such interface choices as potentially manipulative or privacy-intrusive, particularly where they encourage prolonged engagement. The analysis of 'addictive behaviour' (para 47) is especially concerning, as this is a complex scientific topic, and the guidelines provide no objective foundation for this analysis.

This substantive overreach is compounded by regulatory ambiguity as to which types of dark patterns would fall under the DSA's provisions on deceptive design and user protection, and which would instead be assessed under the GDPR's data protection principles. This overlap risks regulatory ambiguity and conflicting supervision, as both Digital Services Coordinators (under the DSA) and Data Protection Authorities (under the GDPR) could claim jurisdiction. Greater clarity is

therefore needed to ensure consistent enforcement, legal certainty, and room for legitimate user experience design.

7. PROFILING USING SPECIAL CATEGORIES OF DATA (ARTICLE 26)

The Guidelines state that the processing of special categories of data, including profiling based on these data, is subject to a specific legal regime as set out in Article 9 GDPR. Processing of such special categories of data is prohibited in principle, unless it relies on specific derogations, as set out in Article 9(2) GPDR. The scope of the special categories of data under Article 9(1) GDPR is very broad. It may include data derived or inferred from profiling activity or indirect disclosure of such data. Moreover, it does not matter if the information revealed by the processing operation in question is correct and if the controller is acting with the aim of obtaining information that falls into that category.

We believe the EDPB's guidelines in paragraphs 72-76 adopt an overly strict interpretation of profiling and inferences, in relation to advertising. The Guidelines appear to take a zero-risk approach to any data field that may infer a special category data point; rather than paying regard to whether the controller had any intent to make inferences. This overly strict interpretation could have a significant impact on the delivery of advertising based on the viewing of online content that could at a stretch indicate tangentially a special category of data, e.g. viewing content about a kosher bakery does not mean a controller would make inferences regarding the user's religion.

As a separate but related point on Article 9, we would also urge the EDPB to provide certainty that biometric processing for the sole purpose of age estimation—as distinct from unique identification—does not constitute special category data.

8. RECOMMENDER SYSTEM (ARTICLES 27 AND 38)

The guidelines suggest that profiling-based recommender systems are subject to strict rules under the GDPR and DSA, requiring at least one non-profiling option that is presented equally without nudging users. This is a significant concern, as the guidelines' presumption that recommender systems trigger Article 22 (para 84) is legally unfounded. The mere presentation of content does not meet the high threshold of a 'legal or similarly significant effect' as established by foundational

data protection guidance, which reserved this for decisions with profound or discriminatory impacts.

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 not only significantly exceeds the requirements of the DSA but it also overlooks the clear user benefits of these systems (as noted in para 81).

Such prescriptive requirements risk undermining innovation in interface design and content curation, which are core elements of service differentiation and user engagement strategies. They would also likely contribute to "choice fatigue" in circumstances where recipients of the service are already required to make several selections when using a service under existing regulatory frameworks, which include the GDPR and the DSA's own transparency and control provisions.

9. Risk assessment (Article 34)

The guidelines conclude that providers of VLOPs and VLOSEs are obliged under Article 34 DSA to carry out a risk assessment for systemic risks including, inter alia, risks to the protection of personal data according to Article 8 of the Charter which the GDPR reflects in secondary law. If there are systemic risks, a DPIA according to Article 35 GDPR is likely to be mandatory.

We believe that the Guidelines should clarify that a data protection impact assessment (DPIA) is only required if the GDPR's threshold is met, even in the context of the DSA's Article 34 risk assessment.

The concept of systemic risk to the protection of personal data in the DSA is not identical to the threshold for a DPIA set out in article 35 GDPR.

10. Conclusion and policy suggestions

The EDPB's draft Guidelines on the interplay between the DSA and the GDPR constitute an important step toward ensuring coherence within the EU's digital regulatory framework. Nevertheless, as currently formulated, the Guidelines risk generating legal uncertainty, overlapping competences, and disproportionate

compliance burdens that could weaken both the protection of fundamental rights and the overall effectiveness of the Digital Single Market.

To safeguard the complementarity of the DSA and the GDPR, the final Guidelines should reaffirm clear institutional boundaries, adopt a proportionate and risk-based approach, and provide practical, predictable guidance to all stakeholders. Establishing such clarity will be essential to promote regulatory consistency, uphold user protection, and sustain innovation and competitiveness within Europe's digital economy. It should also take into consideration the outcome of the proposed DFA regulation that aims to harmonize and strengthen consumer-protection rules across digital business models.

Against this background, the following recommendations outline key measures to enhance legal certainty, proportionality, and institutional integrity in the final version of the Guidelines.

Ensure Legal Certainty and Coherent Cooperation

A predictable regulatory environment is essential for the Digital Single Market. The EDPB's overlapping guidance creates uncertainty, discourages investment, and burdens compliance, especially for SMEs. Clear, consistent, and practical guidance is needed. To achieve this, the EDPB and the European Board for Digital Services (EBDS) should establish formal cooperation and consistency mechanisms to harmonise the application of the DSA and GDPR and provide legal certainty for all stakeholders.

Promote Proportionality and Balance of Rights

Data protection should not be treated as an absolute right. In line with Recital 4 GDPR and CJEU case law, it must be balanced with other fundamental rights — such as freedom of expression, access to information, and the freedom to conduct a business. The Guidelines should explicitly recognize this need for balance, ensuring that privacy measures do not unduly limit online safety mechanisms or other legitimate objectives of the DSA.

Respect Institutional Mandates and Competences

The EDPB must focus on data protection issues strictly within its mandate, avoiding overreach into areas governed by the DSA, such as systemic risks, addictive design, or content moderation rules. Each authority — the EDPB, DSCs, and the EBDS — should operate within its defined competence to preserve institutional integrity and prevent conflicting or duplicative enforcement.