The Association of Community Internet Services (ASIC - www.lasic.fr), established in 2007, is the first French organization to bring together stakeholders in the collaborative web sector. As the main contact for public authorities, the association is a space of reflection and exchanges on topics related to the regulation of digital activities. As such, it acts as a regular meeting place between representatives of civil society, Internet users, digital service companies and public decision-makers.

ASIC is grateful to the European Data Protection Board for the opportunity to contribute to the guidelines on the interplay between the DSA and the GDPR.

General Observations and Need for Coherence

ASIC appreciates the EDPB's efforts to harmonize the enforcement and application of the Digital Services Act (DSA) and the General Data Protection Regulation (GDPR). We agree that a **coherent interpretation** of these two frameworks is essential. However, the current draft Guidelines would possibly introduce significant legal uncertainty by failing to establish necessary consistency protocols and by offering interpretations that are operationally impractical and venture beyond the EDPB's core mandate.

We note with concern the procedural basis upon which these Guidelines were developed, as it is unclear whether the EDPB engaged in substantive consultation with national Digital Services Coordinators (DSCs) or the European Board for Digital Services (EBDS). This lack of transparency undermines the goal of inter-regulatory cooperation and contradicts the EDPB commitment as per the recently approved Helsinki Statement.

Key Areas Requiring Immediate Revision

A. Regulatory Cooperation and Risk of Duplicative Enforcement

The Guidelines correctly identify that neither the DSA nor the GDPR provides an explicit duty of cooperation between authorities. Yet, they fail to propose the formal mechanisms required to ensure consistency and prevent the risk of double and redundant jeopardy.

Without clear, formal protocols, intermediary service providers face the unacceptable possibility of duplicative proceedings and inconsistent enforcement actions launched by both data protection authorities (DPAs) and DSCs for the same underlying conduct.

Furthermore, there is a substantial risk that certain data protection authorities may attempt to leverage the DSA framework to enforce the GDPR, thereby circumventing the established procedural safeguards and competencies defined by the GDPR itself. This concern is heightened by recent actions, such as those by the Berlin DPA, which appear to attempt to apply the DSA's notice-and-action framework (designed for manifestly illegal content) to complex data protection matters that require the GDPR's own rigorous procedural standards. The EDPB should mandate a clear delineation of enforcement competencies to respect the distinct purposes and procedures of both regulations.

B. Misapplication of Automated Decision-Making (Article 22 GDPR)

The EDPB's interpretation regarding automated content moderation systems is disconnected from operational realities. This disconnect threatens to subvert the DSA's core objectives, creating an unworkable framework that may backfire on its intended goals.

1. High Threshold Ignored: The Guidelines suggest that actions taken to detect and remove illegal content may qualify as automated decisions under Article 22 of the GDPR. This position is asserted without sufficient analysis of the high threshold requiring a decision to produce "legal or similarly significant effects". Most content moderation actions are fundamentally about enforcing a provider's terms and conditions, which generally do not rise to the level of having a legal or similarly significant effect contemplated by the GDPR.
2. Impracticality of Data Exclusion: The statement that such content moderation actions "should not involve any processing of personal data" (paragraph 14) sets an unrealistic expectation. This ignores the necessary operational realities involved in training and deploying effective automated content moderation systems.

C. Overreach on Recommender Systems and Deceptive Design

1. Recommender Systems Scope

The definition of a "recommender system" provided in the Guidelines (paragraph 80) is overly expansive and risks inadvertently capturing standard functionalities, such as organic search rankings, that should be considered outside the intended scope of the DSA.

The assertion that the presentation of specific content through a recommender system could constitute a "decision" under Article 22(1) GDPR is presented without adequate justification, contradicts the Article 29 Data Protection Working Party Guidelines and indicates a misunderstanding of how these technical systems operate. Moreover, the Guidelines appear to introduce new obligations not supported by the DSA text, such as a prohibition on "nudging" users towards specific recommender system options, which exacerbates legal uncertainty.

2. Deceptive Design Patterns and Mandate

The EDPB's expansive approach to "deceptive design patterns" ventures significantly beyond its data protection mandate and expertise.

Specifically, the reference to "addictive behaviour" as a source of systemic risk (paragraphs 46 and 47) is concerning, as online addiction is a complex and nuanced topic that falls outside the EDPB's data protection remit. By designating common and legitimate interface features as inherently deceptive without requiring contextual, case-by-case assessment, the Guidelines risk mischaracterizing standard design practices that enhance user experience and could potentially stifle innovation.

D. Practical Gaps in Compliance Guidance

It seems to ASIC that the Guidelines do not provide essential clarity in several key compliance areas:

1. Transparency Conflict: The document highlights a direct conflict between the DSA's transparency obligations (where information may be provided after a processing of personal data has occurred) and the GDPR's requirement to provide information at the time of collection. However, the Guidelines offer no clear, harmonized guidance on how providers are meant to reconcile these distinct legal requirements, creating significant operational challenges.
2. Special Category Data (SCD): There is insufficient substantive guidance on the processing of special categories of personal data, which is often necessary for providers to discharge core DSA obligations, such as illegal content detection. Although the Guidelines acknowledge that automated systems involving SCD could trigger Article 22 GDPR, they fail to offer the necessary substantive commentary on the appropriate special conditions for such processing under Article 22(4) and Article 9. Besides, broad interpretation of "inference" risks classifying almost any data as a 'special category,' which is an unworkable standard. The EDPB should clarify that Article 9's high protections are triggered only by a two-part objective test: a demonstrable intent to reveal SCD and an actual inference by the controller.

E. Age Assurance and Protection of Children

On age assurance, it seems to ASIC that the proposed approach may conflict with other existing legal requirements.

The guidance to "avoid age assurance mechanisms that enable unambiguous online identification" (paragraph 93) is too restrictive and neglects scenarios where such detailed verification is necessary under other legal regimes. Furthermore, the recommendation that providers should not "permanently store the age or age range" (paragraph 94) can be problematic in practice, for instance when retaining this data can be a proportionate measure required to ensure a user continues to receive age-appropriate experiences as they transition into different age categories. We would also encourage the EDPB to provide certainty that biometric processing for the sole purpose of age estimation, as distinct from unique identification, falls outside the scope of Article 9.