INATBA
International Association
for Trusted Blockchain Applications

Response to the EDPB Guidelines 03/2025 on the Interplay Between the Digital Services Act (DSA) and the General Data Protection Regulation (GDPR)

October 2025

On behalf of the INATBA Privacy Working Group, we welcome the adoption of the Guidelines 3/2025 on the interplay between the DSA and the GDPR, the first EDPB guidelines explicitly addressing cross-framework interactions, now open for public comment (12 Sept – 31 Oct 2025).

As continuity with our June 2025 feedback, we reiterate our commitment to risk-based, technology-neutral guidance, with practical, implementation-ready tools for SMEs and OSS builders (PETs, layered architectures, functional erasure).

Our Key Positions

1. No lex specialis override; GDPR legal bases still required. We support the Guidelines' clarification that the DSA does not derogate from the GDPR; DSA-driven processing must rest on a valid Art. 6(1) GDPR basis (often 6(1)(c) or 6(1)(f) depending on context), respecting principles incl. minimization and transparency.

2. Notice-and-Action (Arts. 16–17 DSA) & appeals (Arts. 20, 23). Channels should allow anonymous/pseudonymous reports unless identification is necessary; notifiers should be informed if their identity will be disclosed to affected users; GDPR rights remain intact including Art. 12-16 GDPR. The affected users may – independently from Art. 17 DSA – inquire the identity of an institutional trusted flagger from the platform according to Art. 15 GDPR. The EDPB notes that notifiers process personal data. When they are institutions like trusted flaggers, Art. 14 GDPR applies and they have to disclose to the data subjects that they have processed their personal data meaning that they have flagged their content. This duty might be delegated to the platform, particularly if trusted flagger and platform are considered joint controllers.

3. Recommender systems (Arts. 27, 38). Options must be presented equally (no nudging toward profiling); while a non-profiling option is active, platforms must not continue collecting/processing data to profile the user; in some cases, content presentation can be an Art. 22 GDPR decision.

4. Advertising transparency & sensitive data (Art. 26). DSA ad transparency is ex post, whereas GDPR Art. 13 transparency is ex ante; the DSA's ban on using special-category data for profiling-based ads applies even if a GDPR legal basis and Art. 9(2) derogation exists.

5. Protection of minors (Art. 28). Articles 28(1)–(2) DSA may ground Art. 6(1)(c) GDPR if and only if processing is necessary and proportionate; providers should avoid age-assurance that enables unambiguous identification or permanent storage of age.

6. Systemic-risk duties for VLOPs/VLOSEs (Arts. 34–35). Strong minimization and privacy-by-design/default contribute to mitigation; where risks are identified, a DPIA is likely mandatory.

7. Codes of conduct & coordination. We support clarifying the relationship between DSA codes and GDPR Art. 40 codes, with appropriate DPA involvement; we also endorse the call for sincere cooperation among DSCs, the Commission, and DPAs to avoid inconsistency and ne bis in idem risks.

Web3 / Digital-Assets Considerations We Ask to Make Explicit in the Final Text

- Scope mapping to "online platforms". Many Web3 actors meet the DSA definition of online platform, hosting services that, at a user's request, store and disseminate information to the public, including NFT marketplaces, DAO/community forums, public IPFS/Arweave gateways, and certain dApp/front-end listing and ranking interfaces. We request explicit examples covering these cases.

- Privacy-preserving Notice-and-Action. Encourage privacy-by-default forms, minimal telemetry, and clear disclosure whenever notifier identity may be revealed, consistent with GDPR duties.

- Recommenders in asset marketplaces. Clarify when ranking/curation may constitute Art. 22 decisions, and what concise explanations and non-profiling modes suffice without revealing IP.

- Ad transparency in token/airdrop campaigns. Distinguish ex-post DSA disclosures from ex-ante GDPR notices in mixed on/off-chain campaigns. European Data Protection Board

- Age-assurance for minors. Promote low-intrusion methods and no-retention practices, avoiding unambiguous identification or permanent storage of age.

Practical Tools We Will Provide (Ready on Request)

Building on our June submission's templates and PET-forward approach, layered architectures, functional erasure, ZKPs/selective disclosure, we stand ready to attach: a DSA→GDPR legal-basis matrix; reusable DPIA modules (recommenders, ads, notice-and-action); a "non-profiling mode" policy (UX and telemetry controls); and

Process And Next Steps

We appreciate that the consultation remains open until 31 October 2025 and intend to collaborate with stakeholders to provide concrete implementation examples from Web3 platforms before submission closes.

INATBA
International Association
for Trusted Blockchain Applications

European Data Protection Board

We thank the EDPB for advancing clarity across the DSA and GDPR and remain available to discuss sector-specific codes of conduct and joint legal-technical points of contact to operationalize the duty of sincere cooperation.

For more information, you can follow up with us at privacy-wg-cochair@inatba.org.

This response is supported by the following INATBA Members:

Gabi Urrutia, Halborn	Ismael Arribas and Limara Haque, KUNFUD	Prof. Dr. Ingrid Vasiliu-Feltes, EU Blockchain Observatory and Forum
Harris Niavis, Inlecom	Prof Joyce O'Connor, INATBA Academic Advisory Board	Jörn Erbguth, EU Blockchain Observatory and Forum