Anu Talus

Chair of the European Data Protection Board

Ms Ursula von der Leyen

President of the European Commission

Ms Henna Virkkunen

Executive Vice-President for Tech Sovereignty, Security and Democracy

Mr Michael McGrath

Commissioner for Democracy, Justice, the Rule of Law and Consumer Protection

European Commission
Rue de la Loi 200
1049 Brussels, Belgium

Brussels, 12 November 2026

by e-mail only

Subject: Need for an EU legal basis enabling structured cross-regulatory cooperation and information sharing for digital regulation

Dear President von der Leyen,

Dear Executive Vice-President Virkkunen,

Dear Commissioner McGrath,

At its high-level meeting in Dublin on 16–17 July 2026, the European Data Protection Board (EDPB) discussed how to deepen consistency and cooperation in enforcement, including across regulatory frameworks applicable to the digital economy. In that context, EDPB members agreed to call on the European Commission to consider establishing a clear legal basis for information sharing among regulators with different mandates[1].

The EDPB considers that such an initiative is now necessary in order to provide greater legal certainty for exchanges of information, including confidential information, that may be relevant for enforcement in the respective areas of competence of different regulators, to remove barriers to practical cooperation, and to improve the coherent application of Union law in the digital environment.

[1] European Data Protection Board, "EDPB calls for legal basis for cross-regulatory information sharing", news item, 17 July 2026, available at: https://www.edpb.europa.eu/news/edpb-calls-for-legal-basis-for-cross-regulatory-information-sharing_en

1. Context: an increasingly interlinked digital regulatory landscape

The EU digital regulatory framework has become significantly more complex and interdependent. The same conduct by companies may simultaneously fall within the scope of several legal instruments and competent authorities, including data protection authorities, consumer protection authorities, competition authorities, digital services regulators, market surveillance authorities, media regulators, and other bodies tasked with enforcing Union law.

In this increasingly complex regulatory landscape, effective supervision requires more than general exchanges of views or policy-level alignment only[2]. Authorities also need to be able to exchange information relating to specific cases where the same underlying facts are being assessed from different legal perspectives. This is particularly important where such information may materially assist another authority in exercising its powers and competences.

The EDPB positively notes that examples of such cooperation are gaining traction. These developments show a growing awareness among authorities that the effective application of Union law requires dialogue across regulatory fields. However, cooperation remains too often dependent on ad hoc arrangements, institutional goodwill, and varying national practices, rather than on a clear and reliable legal framework.

2. The current gap: no sufficiently clear legal basis for systematic exchanges between different regulators

The EDPB recognises the useful role played by existing cooperation platforms, including the High-Level Group under the DMA, in fostering dialogue across regulatory fields[3]. However, the practical realities of enforcement increasingly point to the need for a clearer and more structured legal framework for the exchange of information in individual cases.

While the GDPR and the Procedural Rules Regulation provide legislative bases for information sharing between data protection authorities[4], there are still no systematic and sufficiently detailed provisions in EU legislation for exchanges with other regulators, especially where confidential information is concerned.

This legal uncertainty has practical consequences. The EDPB has already encountered situations in which data protection authorities were permitted to receive information from another national regulator, but were prohibited from sharing that information with their counterparts in other Member States, thereby effectively preventing coordination between data protection authorities and undermining a consistent approach. *The EDPB also notes the lack of clear rules governing cross-regulatory cooperation in the context of enforcement, including in relation to the professional secrecy restrictions laid down in Article 54(2) GDPR.* [5]. As a result, authorities face uncertainty as to what may lawfully be shared, with whom, under

[2] EDPS, *Digital Clearinghouse 2.0* note, para. 59.

[3] See Regulation (EU) 2022/1925 (Digital Markets Act), OJ L 265, 12.10.2022, p. 1, Art. 40; Commission Decision of 23 March 2023 on setting up the High-Level Group for the Digital Markets Act, C(2023) 1833 final.

[4] See GDPR, Arts 57(1)(g), 60(1), (3) and (12), 61(1) and 67 (Regulation (EU) 2016/679, OJ L 119, 4.5.2016, p. 1); Regulation (EU) 2025/2518 laying down additional procedural rules on the enforcement of Regulation (EU) 2016/679, OJ L, 2025/2518, 12.12.2025, Arts 9 (relevant information to be exchanged under Art. 60(1) and (3) GDPR), 10 (summary of key issues), 19(3) (preliminary findings), 25(7)–(8) (confidential information) and 26 (cooperation file).

[5] Also see, for example, Article 84 DSA, Article 36(4) DMA, Article 37(16) DA, Article 26(6) DGA, and Article 70 AI Act.

what conditions, and subject to which safeguards, even where several regulators are dealing with the same factual situation under different legal frameworks.

3. Why this matters in practice for regulators

The absence of a clear legal basis in EU law is not an abstract concern. It already affects concrete cases and creates risks of fragmentation, inefficiency and inconsistent enforcement, together with legal uncertainty for businesses.

Several recent cases involve the parallel examination of the same underlying practices under different legal frameworks, including under the GDPR, the DSA, consumer protection law and the DMA[6]. A prominent example concerns “pay-or-consent” models, under which users are required either to pay for access to a service or to accept behavioural advertising. Such models have been scrutinised simultaneously under data protection law, consumer protection law, the DMA and the DSA[7]. This illustrates how a single business practice can trigger parallel proceedings across multiple EU regulatory regimes, making effective cooperation between regulators increasingly necessary.

At the same time, existing legislative solutions at EU level remain partial. The Directive (EU) 2024/2831 on improving working conditions in platform work expressly provides that data protection supervisory authorities and other national competent authorities shall, where relevant, cooperate and exchange relevant information with each other, including information obtained in the context of inspections or investigations[8]. The Political Advertising Regulation relies on a different and more indirect formulation, requiring Member States to ensure cooperation and coordination among relevant national authorities[9]. The AI Act, as amended by the AI Omnibus, contains a direct mutual-assistance and information-exchange duty between market surveillance authorities and bodies enforcing Union fundamental-rights law[10].

Taken together, these examples show both the growing practical need for cross-regulatory exchanges and the fragmentation of the legal bases currently available for them.

A clear legal basis for cross-border information-sharing among regulators with different competences would promote greater consistency, provide regulated entities with clearer legal guidance, and improve enforcement efficiency.

4. Risks resulting from the current situation

In the absence of a clear cooperation framework, interplaying mandates risk leading to fragmented enforcement in practice. Authorities may reach diverging conclusions on closely related conduct or apply similar legal standards inconsistently to the same factual situation. Such outcomes undermine legal certainty and weaken the effectiveness and credibility of the EU’s digital framework.

---

[6] See, for example, the cases mentioned in EDPS, *Digital Clearinghouse 2.0* note, para. 30.

[7] See EDPS, *Digital Clearinghouse 2.0* note, para. 32.

[8] Directive (EU) 2024/2831 on improving working conditions in platform work, OJ L, 2024/2831, 11.11.2024, Art. 24(2); see also recital 73.

[9] Regulation (EU) 2024/900 on the transparency and targeting of political advertising, OJ L, 2024/900, 20.3.2024, Article 22(7)

[10] Regulation (EU) 2024/1689 (AI Act), OJ L, 2024/1689, 12.7.2024, Art. 77(1)–(1b), as amended by Regulation (EU) 2026/1744 (Digital Omnibus on AI), OJ L, 2026/1744, 24.7.2026, Art. 1, point (34).

Fragmentation may also result in enforcement gaps. Where several authorities are competent in parallel, there is a risk that each authority assumes that certain aspects of harmful conduct fall exclusively or primarily within another authority's remit. Conversely, parallel proceedings might be pursued independently, leading to duplication of investigative efforts, repeated collection of the same evidence, disproportionate cumulative burdens for regulated entities, and possible tensions with the principle of double jeopardy (*ne bis in idem*)[11].

5. The EDPB's request to the Commission

The EDPB invites the Commission to consider drafting a legislative proposal establishing a clear basis in EU law for cross-regulatory cooperation and information sharing among competent authorities responsible for enforcing Union rules applicable in the digital economy. In particular, such a proposal should ensure that information may be shared not only among regulators with different mandates at national level but also across borders between competent authorities in different Member States.

In the EDPB's view, any such legislative initiative should establish a clear and sufficiently detailed framework, identifying the authorities concerned, the scope and purposes of cooperation, and the conditions under which relevant information may be shared and used for enforcement purposes. It should also provide for appropriate safeguards governing such exchanges, including rules ensuring compliance with professional secrecy obligations, confidentiality, respect for procedural rights, and practical mechanisms enabling structured and, where appropriate, coordinated cooperation[12]. This legal basis may be complemented by provisions of administrative Member State law where appropriate.

Such an initiative would not necessarily require reopening the substantive provisions of the various instruments making up the EU Digital regulatory framework, in the same way that giving consumers collective redress rights in a directive did not require reopening the EU legislation that consumers could invoke[13]. A horizontal legal basis for cooperation and information sharing could already make a significant contribution to reduce enforcement fragmentation, increase legal certainty, and ultimately contribute to a more effective application of Union law in the digital economy.

The EDPB remains at the Commission's disposal to contribute its expertise to any further reflection or preparatory work on this issue.

Yours sincerely,

Anu Talus

[11] Case C-117/20 *bpost SA v Autorité belge de la concurrence* EU:C:2022:202, paras 33–35, 51-52, and 58.
[12] On the same topic, see EDPS, *Digital Clearinghouse 2.0* note, para. 59-61.
[13] Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC OJ L 409, 4.12.2020, p. 1–2

Copy to:

Mr Roberto Viola, Director-General, DG CNECT;

Ms Ana Gallego Torres, Director-General, DG JUST.