30 October 2025

Response by the Centre for Information Policy Leadership to the EDPB draft guidelines on the interplay between the Digital Services Act (DSA) and the General Data Protection Regulation (GDPR)

The Centre for Information Policy Leadership (CIPL)[1] welcomes the opportunity to respond to the European Data Protection Board's (EDPB) public consultation on the draft guidelines[2] on the interplay between the Digital Services Act (DSA)[3] and the General Data Protection Regulation (GDPR)[4].

Clear, concise, and practical regulatory guidance is essential for organisations, as it provides the legal certainty needed to navigate an increasingly complex and overlapping regulatory landscape.[5] This is particularly important in cases of legislative overlap, where the jurisdictions and competencies of multiple regulators may intersect.

CIPL supports the clarification the draft guidelines make, that the DSA does not act as *lex specialis* to the GDPR, and the explicit reference to existing Court of Justice of the European Union (CJEU) case law that European regulations of the same hierarchical status should be interpreted in a manner that ensures consistency and coherence.

Below, CIPL has identified several areas of attention where draft guidelines would benefit from greater clarity.

[1] **The Centre for Information Policy Leadership (CIPL)** is a global privacy and data policy think tank within the Hunton law firm that is financially supported by the firm, 85+ member companies that are leaders in key sectors of the global economy, and other private and public sector stakeholders through consulting and advisory projects. CIPL's mission is to engage in thought leadership and develop best practices for the responsible and beneficial use of data in the modern information age. CIPL's work facilitates constructive engagement between business leaders, data governance and security professionals, regulators, and policymakers around the world. For more information, please see CIPL's website at www.informationpolicycentre.com. Nothing in this document should be construed as representing the views of any individual CIPL member company or Hunton. This document is not designed to be and should not be taken as legal advice.

[2] European Data Protection Board, *Guidelines 3/2025 on the Interplay between the DSA and the GDPR* (public consultation), September 12 2025, available at https://www.edpb.europa.eu/news/news/2025/interplay-between-dsa-and-gdpr-edpb-adopts-guidelines_en.

[3] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (Digital Services Act), OJ L 277, 27 October 2022, available at http://data.europa.eu/eli/reg/2022/2065/oj.

[4] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), OJ L 119, 4 May 2016, available at http://data.europa.eu/eli/reg/2016/679/oj.

[5] Centre for Information Policy Leadership (CIPL), *The Impact of Digital Advertising on Europe's Competitiveness: A Study on the Role of Digital Advertising in Europe*, March 2025, available at cipl_public_first_the_impact_of_digital_advertising_eu_competitiveness_study_mar25_.pdf.

In the context of the EDPB draft guidelines, CIPL provides the following recommendations:

- Adapt the draft guidelines to ensure they are **accessible, concise, clear, and practical**.
- Ensure that the draft guidelines reflect **cross-regulatory collaboration** and provide transparency regarding any consultative process with other competent regulators undertaken by the EDPB prior to their issuance.
- Clarify the **interpretation of automated decision-making (ADM) provisions** in the context of these draft guidelines **without extending** such interpretation **beyond what is legally justified**.
- Provide **concrete, practical guidance on the transparency requirements** under the GDPR and the DSA, illustrating how these can be operationalised in a compliant and effective manner.
- Clarify that the principle of **data minimisation should not be interpreted** so **narrowly** as to restrict necessary and lawful processing of personal data.
- Encourage a **broad and balanced interpretation of the principles of accuracy, fairness, and purpose limitation** to avoid inadvertently hindering innovation.
- Promote a **risk-based approach to the retention of minors' age data**, particularly when pseudonymised, to support age-appropriate online experiences.
- Ensure **consistency with the European Commission's Guidelines on the Protection of Minors** under Article 28 of the DSA.
- Provide clear and harmonised regulatory **guidance** on the **appropriate conditions for processing special categories of personal data**.

I. General observations

1. The EDPB should provide clear, accessible, and practical guidelines within its competence.

The draft guidelines should aim to be concise and accessible, providing practical examples that support controllers, processors, and national data protection authorities in their assessment of specific cases, thereby promoting a consistent interpretation of the law. The draft guidelines would benefit from a clearer focus on the instances of overlaps between specific articles of the DSA and the GDPR, to provide the necessary clarity around the processing of personal data in the context of the DSA. For example, we note the helpful clarification in paragraph 17, that legitimate interest under Article 6(1)(f) can serve as a suitable legal basis for the own initiative investigations of intermediary service providers under Article 7 DSA.

At the same time, CIPL reiterates the need for more in-depth guidance on the delineation between the GDPR Data Protection Impact Assessment (DPIA) (Article 35) and the fundamental rights impact assessment under the DSA (Article 34), as clear differentiation would help avoid duplication and ensure that regulatory focus remains targeted and effective.

In addition, the draft guidelines fail to address the processing of personal data in the context of obligations under the DSA for data sharing with third parties.

The EDPB should, however, refrain from providing its own interpretation of individual articles of the DSA. For example, paragraphs 43 – 47 of the draft guidelines consider at length deceptive design patterns under Article 25 DSA. This is a complex and contested concept and falls primarily within the remit of other regulators. The draft guidelines' analysis of concepts like "addictive behaviour" is furthermore not explained and lacks a clear evidential foundation. For example, the draft guidelines refer to "infinite scrolling" or "autoplay" as "deceptive design patterns" (and therefore classify them as dark patterns),

thereby seemingly conflating dark patterns with consideration for "addictive design". However, there has been no indication by the European Commission ('the Commission') that these (or similar) features fall within the scope of "dark patterns" under the DSA.

Article 25(2) also explicitly excludes personal data and consumer protection practices from the scope of the prohibition in Article 25(1) DSA. Any guidance should, therefore, be developed only in close coordination with the authorities competent in these domains to ensure consistency, clarity, and legal coherence. Without clear evidence of a consultative process with the Commission, European Board for Digital Services (EBDS) or national Digital Services Coordinators (DSCs), an interpretation of the DSA by the EDPB will lead to fragmentation rather than a coherent interpretation of GDPR and DSA.[6]

2. The importance of cross-regulatory collaboration.

CIPL supports the emphasis the EDPB places on cooperation between competent authorities and the duty of sincere cooperation, which will necessarily include national authorities competent under the DSA that are not data protection authorities. CIPL strongly supports the close collaboration of competent authorities, ideally in the form of joint guidelines similar to the recent joint Digital Markets Act (DMA) and GDPR guidance or upcoming Artificial Intelligence (AI) guidelines with the AI Office, in order to ensure coherent interpretation and application.[7]

CIPL regrets that the draft guidelines provide no transparency on the extent to which the EDPB engaged in any consultative process prior to the issuing of the draft guidelines with the principal enforcers of the DSA. This siloed approach does not align with the principle of cross-regulatory cooperation enshrined in the EDPB's Helsinki Statement[8] and carries the risk of undermining legal certainty. To preserve coherence between frameworks, greater clarity would be welcome to ensure that DSA mechanisms are not applied to issues that are more appropriately addressed under the GDPR.

We would therefore welcome proposals from all stakeholders towards a framework within which future consultation would take place to ensure legal coherence and prevent instances of *ne bis in idem*.[9]

[6] See for example the clear delineation of interpretive competence in the Joint Guidelines on the Interplay between the Digital Markets Act and the General Data Protection Regulation, paragraph 9, available at https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2025/joint-guidelines-interplay-between-digital_en.

[7] European Data Protection Board (EDPB), *Joint Guidelines on the Interplay Between the Digital Markets Act and the General Data Protection Regulation* (public consultation), 9 October 2025, available at https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2025/joint-guidelines-interplay-between-digital_en.

[8] European Data Protection Board. *The Helsinki Statement on Enhanced Clarity, Support and Engagement*. July 3, 2025, https://www.edpb.europa.eu/news/news/2025/helsinki-statement-enhanced-clarity-support-and-engagement_en.

[9] In the reverse, when a DSA regulator is engaged, when it comes to matters in scope of the GDPR, the one stop shop should remain central.

II. Specific Observations

1. Further clarification of the threshold under which specific actions are considered automated decision-making (ADM) under Article 22 GDPR.

The EDPB proposes that "it cannot be excluded"[10] that actions such as:

- detecting and removing illegal content under Article 7 DSA;
- advertising on online platforms under Article 26(1) DSA;
- and the provision of specific content via recommender systems under Articles 27 and 38 DSA,

could constitute automated decision-making (ADM) under Article 22 GDPR.

CIPL believes that this interpretation may broaden the application of Article 22 GDPR beyond what is legally justified.

The notion of "legal" effect and a "similarly significant" effect in Article 22 GDPR requires a high threshold to cover only ADM producing an impact on someone's legal rights or something that affects a person's legal status or rights under a contract, or a decision with similar effects and significance. This covers, for example, (i) ADM affecting accrued legal entitlements of a person or public rights, (ii) ADM affecting an individual's eligibility and access to essential services, admission to a country or to a university, or (iii) ADM to apply tax deductions.[11]

The former WP29 Guidelines on ADM provide useful context, noting that:

"For data processing to significantly affect someone, the effects of the processing must be sufficiently great or important to be worthy of attention. In other words, the decision must have the potential to:

- *significantly affect the circumstances, behaviour, or choices of the individuals concerned;*
- *have a prolonged or permanent impact on the data subject; or*
- *at its most extreme, lead to the exclusion or discrimination of individuals."*[12]

Although the EDPB refers to these guidelines, it does not provide further analysis or sufficient practical examples that would demonstrate how Articles 7, 26(1), 27 and 38 DSA would amount to an effect that would pass the high threshold of Article 22 GDPR. Recital 71 GDPR lists a number of high-risk examples, such as e-recruiting practices without any human intervention or credit refusal. The Advocate General's Opinion in Schufa Case (C-634/21)[13] also considers serious legal or economic consequences for the data

[10] Paragraph 84 of the EDPB guidelines.
[11] Centre for Information Policy Leadership (CIPL), Comments on the Article 29 Data Protection Working Party's "Guidelines on Automated Individual Decision-Making and Profiling", 1 December 2017, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comments_to_wp29_guidelines_on_automated_individual_decision-making_and_profiling.pdf.
[12] Article 29 Data Protection Working Party. Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679, 3 October 2017, available at https://ec.europa.eu/newsroom/article29/items/612053.
[13] Court of Justice of the European Union, Opinion of Advocate General Pikamäe in Case C-634/21, OQ v Land Hessen and SCHUFA Holding AG, March 16, 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62021CC0634.

subject in this context, such as the refusal to grant credit. This is a distinctly higher threshold to the EDPB's consideration of Article 22, such as profiling for general online advertisement, or content removal that is often minor, temporary, and subject to appeal.

2. Further clarification on the interplay of the transparency requirements under the GDPR and the DSA.

The EDPB acknowledges that transparency obligations regarding advertisements under the DSA must be provided in real time,[14] while general transparency obligations under Articles 13 and 14 GDPR require information at the time data is obtained. This distinction means that DSA-mandated information is often provided after personal data processing may have occurred.

CIPL fully supports the emphasis on transparency, recognising it as a fundamental principle that empowers users and builds trust. However, the draft guidelines fall short of providing actual, practical guidance on how to reconcile differing transparency requirements under the GDPR and the real-time, post-processing transparency requirements under the DSA.

CIPL recommends that the EDPB provides clearer, more practical guidance with examples that can demonstrate how both concepts could be approached in a compliant manner. In this context, the EDPB should also engage with stakeholders within the scope of the DSA to better understand the sequence and processes involved in adhering to the DSA transparency obligations.

3. Data minimisation does not mean the absence of personal data processing.

In paragraph 14, the EDPB stresses that personal data use in AI/ML training should be minimised, with providers demonstrating compliance and, wherever possible, such techniques should operate without processing personal data "insofar as possible". CIPL would like to respectfully provide that the aim of the GDPR is not to prevent the processing of personal data.[15] The objective of data minimisation is to limit the unnecessary and excessive collection, processing, and retention of personal data. The focus of the data minimisation principle is on what is *necessary for a legitimate purpose,*[16] to limit the risks of misuse, unauthorised access, and data breaches.

Necessity provides that the processing can only proceed where the objective cannot be equally achieved through less restrictive means. It, therefore, links the processing of personal data to a specific and justifiable purpose. It does not, however, inherently dictate a particular volume of data. A single item of personal data may already be excessive if it is not necessary for the intended outcome. Conversely, processing large volumes of personal data may be entirely appropriate, provided that each data point serves a legitimate and necessary purpose.[17] The CNIL has also rightly acknowledged that "the data

[14] Paragraph 52 of the EDPB guidelines.
[15] Article 1 (3) GDPR.
[16] Paragraph 42 of the EDPB guidelines.
[17] Commission nationale de l'informatique et des libertés (CNIL), "AI and GDPR: the CNIL publishes new recommendations to support responsible innovation", 7 February 2025, available at https://www.cnil.fr/en/ai-and-gdpr-cnil-publishes-new-recommendations-support-responsible-innovation.

minimisation principle does not prevent the use of large training datasets"[18] in the context of AI development.

Furthermore, paragraph 42 of the draft guidelines appears to create a tension between the accuracy principle and the data minimisation principle. Instead, a more flexible, purpose-driven approach that balances privacy with innovation, societal benefits, and economic realities is essential and should be followed.[19] CIPL further stresses that it is not only data minimisation but that the principles of accuracy, fairness, and purpose limitation should all be interpreted in a way that also enables innovation to flourish responsibly.

4. Risk-based and proportionate approach in the storage of minors' age.

The draft guidelines suggest that providers should not permanently store the age or age range of minors as a result of their age assurance process.[20] However, in specific cases, this would be operationally difficult to implement, as it would fragment the age assurance process by constantly re-verifying the age of the minor. This could also result in unnecessary and excessive data processing, undermining the principle of data minimisation.

Furthermore, retaining such data, particularly if pseudonymised, can be a legitimate and proportionate measure necessary to ensure age-appropriate experiences as a user transitions between different age categories and to discharge ongoing obligations under Article 28(1) DSA. It is also contradictory to the intermediary solution[21] (the so-called age verification solution) the EU has already produced. In particular, the age verification solution allows service providers to either request proof on demand or store derived information using a pseudonym for a streamlined experience.

Finally, the draft guidelines should ensure coherence with the recent Guidelines on the Protection of Minors[22] issued by the Commission. In it, the Commission notes that "it is important to distinguish between, on the one hand, the age restriction that limits access to the platform or to parts thereof to users below or above a certain age, and, on the other hand, the age assurance methods that are used to determine a user's age."

The Commission states in several sections of the Article 28 guidelines that platforms should adjust access to features, content or activities based on the evolving capabilities of minors. This would presuppose a record of the age of the minor against which the development of the minor can be measured. The EDPB draft guidelines appear to be creating a tension.

---

[18] Commission nationale de l'informatique et des libertés (CNIL). "AI and GDPR: the CNIL Publishes New Recommendations to Support Responsible Innovation" CNIL, February 7, 2025, https://www.cnil.fr/en/ai-and-gdpr-cnil-publishes-new-recommendations-support-responsible-innovation#:~:text=The%20data%20minimisation%20principle%20does,unnecessary%20processing%20of%20personal%20data.

[19] Recital 4 GDPR also recognises the need to balance data protection with other fundamental rights.

[20] Paragraph 94 of the EDPB guidelines.

[21] European Age Verification Solution, *Overall Architecture - European Age Verification Solution Technical Specification*, March 2025, available at https://ageverification.dev/av-doc-technical-specification/docs/architecture-and-technical-specifications/#26-key-differences-between-the-age-verification-application-and-the-age-verification-functionality-in-the-eudi-wallet.

[22] European Commission, Guidelines on the Protection of Minors, *Shaping Europe's Digital Future*, July 14, 2025, https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-protection-minors.

CIPL supports the work towards further standardisation, such as through a centralised interoperable age assurance solution that streamlines the process and reduces the burden of repeated checks across multiple services for platforms and users. An interoperable system, where age information established in one trusted context could be shared or reused, could simplify the process for all stakeholders significantly. CIPL recognises that such a solution must carefully balance a number of challenges, including privacy, security, competition concerns, cost, and liability.[23] This discussion forms part of the Multistakeholder Dialogue on Age Assurance, launched by CIPL and WeProtect Global Alliance in 2024.[24]

5. Limited guidance on the use of special categories of data.

The draft guidelines offer limited direction on processing special categories of personal data, despite their relevance to fulfilling some DSA obligations. This omission leaves providers without clear regulatory guidance on the appropriate Article 9 conditions for such processing. For example, the draft guidelines do not provide clarification that the processing of biometric data used solely for the purpose of age assurance, as distinct from unique identification, does not constitute a special category of data under Article 9 GDPR.

CIPL invites the EDPB to consider to what extent the substantial public interest condition under Article 9(2)(g) may be an available and appropriate legal basis for processing of personal data for certain obligations under the DSA, given their broad societal importance and provided that adequate safeguards are in place. For example, the DSA requires Very Large Online Platforms (VLOPs) to identify systemic risks (Article 34). This may involve the processing of special categories of data. The draft guidelines could be more specific on whether the processing of special categories data, for the sole purpose of identifying systemic biases and discrimination, could be justified under the substantial public interest (Article 9(2)(g)) basis. This would also be crucial to ensure that VLOPs can meet their Article 35 DSA risk mitigation obligations effectively while adhering to GDPR requirements.

[23] Centre for Information Policy Leadership & WeProtect Global Alliance. (2024, September). *A Multi-Stakeholder Dialogue on Age Assurance: Key Takeaways*, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_weprotectglobalalliance_keytakeaways_multistakeholderdialogue_sep24.pdf.
Centre for Information Policy Leadership & WeProtect Global Alliance. (2024, October–November). *A Multi-Stakeholder Dialogue on Age Assurance – Law and Regulation (Virtual)*, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_weprotect_a_multistakeholder_dialogue_on_age_assurance_law_and_regulation_apr25.pdf.

[24] Centre for Information Policy Leadership & WeProtect Global Alliance. (2024, March). *A Multi-Stakeholder Dialogue on Age Assurance: Key Takeaways (Kick-off Meeting)*, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/key_takeaways_from_a_multi-stakeholder_dialogue_on_age_assurance.pdf.