CENTRE FOR CYBERSECURITY BELGIUM

31, October, 2025

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

The Centre for Cybersecurity Belgium (CCB) wishes to thank the European Data Protection Board (EDPB) for the considerable effort invested in developing these guidelines. We appreciate the EDPB's work in promoting coherence between the Digital Services Act (DSA) and the General Data Protection Regulation (GDPR), which is essential for ensuring legal certainty and effective protection of fundamental rights.

However, we would like to share the following observations and recommendations:

1. Timing and approach

While these guidelines are valuable, their **extensive length and insufficient operational guidance** make them less accessible to the stakeholders who must apply them in practice. By 'insufficient operational guidance', we refer to the fact that the guidelines are written in a highly technical and legalistic tone. While this is understandable given the nature of the subject matter, it makes them harder to interpret and apply in day-to-day situations. A more accessible, human-centered language - with concrete examples and practical steps - would significantly improve their usability for non-experts.

2. Target audience and clarity

It remains unclear who the **intended audience** of these guidelines is: policymakers, supervisory authorities, or providers of intermediary services and online platforms. The current structure and tone appear more suited to **policymakers & people with legal background**, while the DSA itself primarily addresses **service providers** who need clear, operational guidance.

We therefore recommend clarifying the **target group** of the document and revising certain sections for **readability and practical applicability (e.g. recital 2.**could be rephrased for clarity: The DSA sets rules for different types of intermediary service providers (like mere conduit, caching, and hosting services), which involve different levels of personal data processing. This version improves accessibility while preserving the original meaning.)

3. Interplay and scope of the guidelines

Certain sections of the guidelines **extend beyond clarifying the relationship between the DSA and the GDPR**, venturing into substantive policy positions. For instance, the discussion on technologies for voluntary detection of illegal content and age verification (Recitals 14, 93 & 94) includes normative judgments about the reliability and risks of specific tools. These risks pre-empting future regulatory and technical debates. Recital 93 is particularly illustrative, where the EDPB states that age assurance can be achieved without identifying the user and discourages mechanisms involving government-issued IDs,

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister
Rue de la Loi / Wetstraat 18 - 1000 Brussels
www.ccb.belgium.be

based solely on Article 28 DSA. While this reflects legitimate privacy concerns, it also implies a technological preference and prematurely excludes certain approaches. Such determinations should be left to legislative or technical standard-setting bodies/documents, where proportionality, effectiveness, and innovation can be properly weighed.

4. Age verification and protection of minors

To complement the above, we encourage the EDPB to adopt a balanced approach that acknowledges both privacy and technical feasibility. While we support the emphasis on privacy-preserving and proportionate age assurance mechanisms, it is equally important to ensure that these solutions are **technically robust and resistant to misuse**. The assertion that age assurance can occur "without identification of the respective user" (Recital 93) is conceptually valid, but should be qualified by recognising the operational challenges of verifying age without processing at least some personal data. Even privacy-enhancing methods - such as tokenisation, zero-knowledge proofs, device-based estimation, or third-party verification - typically involve some level of data processing. Therefore, any guidance on the DSA-GDPR interplay should also reflect the security dimension of data protection by design and by default, ensuring that age assurance systems are not only privacy-friendly but also effective in practice.

5. Systemic risks and cybersecurity

Articles 34 and 35 DSA refer to the management of **systemic risks**, including those affecting fundamental rights and public security. We recommend that the guidelines explicitly acknowledge **cybersecurity risks** as part of these systemic risks, and encourage cooperation between **Digital Services Coordinators**, **data protection authorities**, and **cybersecurity agencies**.

The CCB previously raised a similar point regarding the Article 28 DSA guidelines: cybersecurity aspects should be **structurally integrated** into the application and oversight of the DSA, particularly concerning systemic risk management.

Furthermore, the principle of **data protection by design and by default** under the GDPR inherently includes **cybersecurity by design** — security and privacy reinforce one another and should be treated as complementary.