Consultation Response by European Digital Rights for the Draft EDPB Guidelines on the Interplay between GDPR and DSA

EDRi welcomes the opportunity to provide feedback on the draft EDPB Guidelines 3/2025 on the interplay between the DSA and the GDPR. Both regulations are crucial pieces of the EU's legal *acquis* to protect fundamental rights in the digital era. Their forceful and consistent application and enforcement is therefore key to protect people's rights.

At the same time, the draft Guidelines risk focusing too narrowly on reconciling the DSA and the GDPR at a procedural level, rather than examining whether certain DSA-driven processing activities are compatible with fundamental rights in the first place. The EDPB should avoid turning this exercise into a compliance mapping for industry and instead adopt a rights-protective reading that challenges unnecessary or disproportionate data processing. In interpreting the interplay between the two instruments, the EDPB should adopt a purpose-driven reading consistent with the GDPR's overarching objective of ensuring a high level of protection for fundamental rights. References to recitals, particularly those addressing fairness, transparency and non-discrimination, should be treated as interpretative anchors rather than optional guidance.

In that light, EDRi would like to provide the following observations for the EDPB's consideration:

Generally, the Guidelines should more explicitly caution against what might be termed 'lawful-basis inflation,' where controllers automatically invoke Art. 6(1)(c) or (f) GDPR for any processing linked to DSA obligations. The EDPB should underline that compliance with the DSA does not in itself render processing lawful or proportionate under the GDPR.

On automated decision-making

We welcome the EDPB's emphasis in paragraphs 17-18 on error rates in machine learning-based content moderation tools, as well as the risks they constitute for people, in particular when applied at scale. We also welcome the draft Guidelines' recognition that online intermediaries become data controllers under GDPR when processing personal data in complying with the DSA's requirements for user-generated online content moderation, and that as such, they have to respect the users' fundamental and GDPR rights as data subjects.

The clarification that Art. 6(1)(f) GDPR is the most relevant legal basis in this context enhances legal certainty and puts the onus on online platforms to demonstrate the legality of their processing of users' personal data. The Guidelines should, however, reiterate that reliance on "legitimate interest" does not exonerate data controllers of their duty to balance necessity and proportionality in the context of automated content moderation decision-taking. While the GDPR does not establish a hierarchy among legal bases, the proportionality principle limits the use of legitimate interest where the processing itself generates or exacerbates the very risks it purports to address. What is more, platforms should not be able to rely on legitimate interest for content moderation under the DSA to circumvent the GDPR's principle of purpose limitation by processing personal data for other purposes such as profiling, content recommendation and curation, ad targeting, or other forms of personalisation.

The necessity and proportionality tests under the GDPR require controllers to show that no less intrusive means could achieve the same objective. Automated moderation or recommender systems that process personal data at scale cannot be presumed necessary when they themselves generate new risks of error, discrimination, or chilling effects on speech. More generally, it is crucial that hosting providers who rely on automated decision-making tools adhere to GDPR standards, including conducting extensive Data Protection Impact Assessments, and where needed, prior consultation with the relevant Data Protection Authority (DPA). For this to work, DPAs need to be sufficiently funded and staffed in order to be able to do their important work effectively. The EU Commission should therefore start using its powers to force each EU Member State to comply with its obligations under the GDPR in this regard.

On unfair design practices

The deployment of deceptive system and interface design has become a quasi-industry standard on many types of digital services, and most notably on Big Tech services. While we advocate for a more horizontal regulatory approach to deceptive and addictive design patterns as part of the upcoming Digital Fairness Act,[1] we welcome the EDPB's clarification in paragraph 45 that already today most such patters are "generally unlawful" under GDPR as far as they involve or lead to processing of personal data. These kinds of design strategies must indeed be considered unfair in principle.

On online advertising

With regard to online advertising transparency, we welcome the EDPB's insistence in chapter 2.4 on the principle of data minimisation and the legal requirement to not disclose any additional personal data to data brokers, ad platforms or similar intermediaries in today's ad tech supply

1 European Digital Rights (EDRi), A Rights-Based Digital Fairness Act: Background Paper on Protecting People from Manipulative Design and Data Exploitation, October 2025, available at https://edri.org/wp-content/uploads/2025/10/DFA_Background_Paper_EDRi_final.pdf.

chain. We also note that the complex interplay between the DSA's transparency requirements and the GDPR's data protection rules can serve as an incentive for online platforms to reduce their reliance on profiling-based ad targeting and the real-time bidding market, and instead seek legal simplicity in ad targeting technology that does not rely on the permanent and intrusive surveillance of their users. The Guidelines should support that legal clarity by acknowledging that most advertising practices based on profiling and real-time bidding today remain structurally[2] incompatible[3] with the GDPR's data minimisation and purpose limitation principles.

We also call on DPAs to require that ad tech intermediaries shall be prevented from accessing additional personal data in the process of forwarding transparency information to users not only through legal agreements but also technical means such as encryption.

On recommender systems

Paragraphs 80-81 unfortunately frames the main reason for the widespread use of recommender systems by online platforms as largely positive: because of their alleged "usefulness in facilitating and optimising access to information for the recipients of the service" and "with the aim of presenting what is most likely to interest users first, or with a view to enhance the quality or diversity of the content presented to users." In addition to these assumptions to be very likely incorrect, we believe it would suit an independent regulatory body better to refrain from this kind of endorsement, or—alternatively—at least also mention the other major reasons for which recommender systems are deployed today: to maximise people's screen time and addiction to social media platforms, to amplify polarising or harmful content, to push consumers into buying more (expensive) products on e-commerce platforms, and—more recently and increasingly likely on some platforms—to manipulate public opinion for political gain for tech billionaires.

Relatedly, and rather than repeating industry claims about usefulness unquestioned, the EDPB should also use the Guidelines to assess whether large-scale behavioural personalisation without consent is compatible with the GDPR's principles of fairness and data minimisation at all.

With regard to non-profiling based recommender systems, we very much welcome the EDPB's clarification in paragraph 87 that VLOPs and VLOSEs should "present both options equally (on first use of the service) and should not nudge recipients of the service to select the option for a recommender system that is based on profiling," which is in line with an ongoing complaint filed

2 Michael Veale, Frederik Zuiderveen Borgesius, Adtech and Real-Time Bidding under European Data Protection Law, German Law Journal (2022), 23, pp. 226–256, available at https://arxiv.org/pdf/2509.08838.

3 Irish Council for Civil Liberties, EU ruling: tracking-based advertising by Google, Microsoft, Amazon, X, across Europe has no legal basis, 14 May 2025, available at https://www.iccl.ie/digital-data/eu-ruling-tracking-based-advertising-by-google-microsoft-amazon-x-across-europe-has-no-legal-basis.

by Bits of Freedom, EDRi and partners against Meta in front of the Digital Services Coordinator (DSC) in Ireland,[4] and corresponding jurisprudence in the Netherlands.[5]

Even more importantly, we strongly welcome the EDPB's clarification that VLOPs and VLOSEs may only use a recommender system based on profiling "after the recipient of the service has chosen this option," which strengthens user choice and consent in relation to recommender system-related data processing. In addition, we welcome the Guidelines' stance that as soon as a user has chosen the non-profiling based recommender system option, VLOPs and VLOSEs "cannot lawfully continue to collect and process personal data to profile the user, for the purposes of future recommendations." These clarifications are crucial to ensure users' fundamental rights are fully protected under the GDPR and the DSA.

Finally, the Guidelines should also reaffirm that under GDPR controllers are required to *prevent* discriminatory effects arising from automated processing and profiling, not merely to minimise them.[6] The DSA's softer language around mitigating bias risks lowering this fundamental standard. The EDPB should explicitly reject any interpretation that dilutes the Charter-level prohibition of discrimination. To meet the GDPR's fairness and accountability standards, platforms must ensure that any human oversight of algorithmic systems is effective and informed. Where the logic of a machine learning system is opaque or unintelligible to its operators, such oversight becomes impossible and cannot be considered compliant with GDPR.

On the protection of minors

We support the DSA's requirements for online platforms to ensure a high level of privacy, safety, and security of minors, on their service. It is therefore welcome that the draft Guidelines set boundaries in chapter 2.6 for the processing of minors' personal data for intrusive technology such as age assurance systems in the context of Art. 28. It is crucial that platform providers are not enabled by the DSA to collect more personal data from young people and invade their privacy even further under the guise of "child protection technology."

We therefore also welcome the draft Guidelines' clarification in paragraph 92 that providers may rely on Art. 6(1)(c) GDPR as a legal basis for processing personal data in their effort to comply

4 European Digital Rights (EDRi), Civil society files DSA complaint against Meta for toxic, profiling-fueled feeds, 15 April 2025, available at https://edri.org/our-work/civil-society-files-dsa-complaint-against-meta-for-toxic-profiling-fueled-feeds.

5 Bits of Freedom, Judge grants Meta limited postponement in Bits of Freedom lawsuit, 28 October 2025, available at https://www.bitsoffreedom.nl/2025/10/28/judge-grants-meta-limited-postponement-in-bits-of-freedom-lawsuit.

6 Douwe Korff, Must all Algorithmic Discrimination be Prevented and Eliminated - or Need it only Be Minimised?, 2 October 2025, available at: https://www.iglobal.lawyer/post/must-all-algorthmic-discrimination-be-prevented-and-eliminated-or-need-it-only-be-minimised.

with Art. 28 DSA only on a case-by-case basis, and only in so far as they are able to demonstrate that "such processing is necessary and proportionate to achieve the goals of Art. 28 DSA." To avoid any misunderstandings, the EDPB should clarify that Art. 6(1)(c) GDPR can only be a valid legal basis in cases where there are no less intrusive means to achieve compliance with Art. 28 DSA, and that simply pointing at the European Commission's political preferences or even the Art. 28 Guidelines is not enough to create a legal basis under GDPR. DPAs should also actively monitor in particular the use of age assurance and user identification systems and related data processing activities under the DSA.

On enforcement gaps

Because the GDPR is *lex specialis* in all matters concerning personal data processing, the EDPB should make clear that the DSA cannot be interpreted as permitting or requiring processing practices that would otherwise contravene the GDPR. Where ambiguity arises, the interpretation that offers the strongest protection of fundamental rights must prevail.

Finally, the Guidelines should address the enforcement gap between DSCs and DPAs. Without clear mechanisms for cooperation and mutual consultation, there is a real risk of fragmented oversight and regulatory forum-shopping by online platform providers. The EDPB should therefore emphasise that DPAs should be meaningfully involved whenever DSA-related processing raises GDPR questions, in order to achieve a consistent interpretation and avoid gaps or delays in enforcement. The EDPB should also emphasise that cooperation mechanisms must ensure that DPAs' interpretations prevail whenever the DSA triggers personal data processing, to prevent dilution of the GDPR's protective standards.

***