amazon EU SARL

Comments on the EDPB's Guidelines 3/2025 on the Interplay Between the DSA and the GDPR

INTRODUCTION

1. Amazon welcomes the opportunity to contribute to the European Data Protection Board's ("**EDPB**") public consultation on the EDPB Guidelines 3/2025 on the interplay between the Digital Services Act ("**DSA**") and the General Data Protection Regulation ("**GDPR**") (Version 1.1) adopted on 11 September 2025 ("**Guidelines**"). We support the EDPB's work in ensuring the coherent interpretation and application of the DSA and the GDPR. In line with the principles of legal certainty and regulatory coherence, the Guidelines should make clear that the DSA and the GDPR are two separate legal regimes subject to different competencies and enforcement.

2. The Guidelines offer valuable clarity in several key areas, particularly in encouraging structured cooperation between regulators, setting out a risk-based and proportionate approach to age assurance, and recognising the parallel application of the GDPR and DSA ad transparency obligations. The emphasis on consultation and cooperation between digital services coordinators under the DSA and supervisory authorities under the GDPR is vital to prevent duplication of effort and regulatory inconsistencies while maintaining each authority's independent enforcement role. This should include ensuring that each authority limits the use of its investigative and enforcement powers, such as information requests, to matters within its own remit. Avoiding intrusive age assurance methods such as government ID checks, unless required, appropriately balances the protection of minors with the preservation of privacy. We support the EDPB's clarification that the DSA's advertising transparency requirements operate independently from the transparency requirements under the GDPR. In particular, the EDPB rightly explains that information under Article 26 DSA may be provided after processing of personal data may have occurred.

3. The Guidelines would, however, benefit from greater clarity by observing a few principles. First, while supporting the need for coherent application of Union legislation, it is important that each authority limits its interpretative statements to the subject matter falling within its jurisdiction. For example, whether a design constitutes a deceptive pattern under the DSA should not be addressed in these Guidelines, but rather by the relevant digital services authorities. Second, where the EDPB, or the Article 29 Working Party before it, has previously issued guidance on a topic, it is important to ensure the Guidelines remain consistent with previous guidance. For instance, the Article 29 Working Party Guidelines on Automated Individual Decision-Making and Profiling ("**WP29 ADM Guidelines**") provide clarity on what constitutes automated decision-making under the GDPR, and the Guidelines, as currently drafted, risk contradicting these established guidelines. Third, the Guidelines should clarify what the rule and the exception are, instead of focusing on edge cases, often with social media use cases in mind. In particular, we have identified the following areas and recommendations to address these issues:

- **Introduction and scope of the Guidelines** (Section 1)

4. Paragraph 6 of the Guidelines provides that the Guidelines do not address any issues around the application of the GDPR arising in the context of the European Commission's delegated regulation under Article 40(13) DSA, nor do the Guidelines cover issues in relation to personal data arising under Article 40 DSA more generally.

5. However, this is subject matter involving the interplay between the DSA and the GDPR that would clearly benefit from clarification. Article 40 DSA specifically refers to personal data but without providing clarification on how risks to the protection of personal data are to be addressed when responding to reasoned requests from the Commission or Digital Services Coordinators, reasoned requests under Article 40(4) from the Digital Services Coordinator, or access requests made by researchers under Article 40(12) DSA. In particular, guidance from the EDPB would be welcome on the interpretation of Article 40(2) DSA in relation to data access by the Digital Services Coordinators and the European Commission, and Article 40(8)(d) DSA, which refers to applications from researchers, where they mention specific data security and

confidentiality requirements to protect personal data, as well as appropriate technical and organisational measures.

- **Voluntary own-initiative investigations and legal compliance in relation to illegal content** (Section 2.1)

6. Whether voluntary own-initiative investigations pursuant to Article 7 DSA qualify as automated decision-making under Article 22(1) GDPR ("**ADM**") is only subject to the provisions of the GDPR as interpreted by the WP29 ADM Guidelines. These provide sufficient clarity on when processing of personal data qualifies as ADM, thus there is no risk of ambiguity to be addressed by the Guidelines. If the EDPB nonetheless considers it necessary to address ADM in the context of the DSA, this should be used as an opportunity to reaffirm, rather than reinterpret, the WP29 ADM Guidelines to ensure consistency and avoid the introduction of conflicting guidance. For example, the Guidelines state that some decisions to remove allegedly illegal content "*could significantly affect recipients of the service whose content is removed"*, without clarifying that this will be the exception as *"the threshold for significance must be similar to that of a decision producing a legal effect"* (emphasis added).[1]

7. We therefore respectfully invite the EDPB to consider the following revisions to paragraph 22 to bring it in line with the WP29 ADM Guidelines:

> "*Depending on the level of automation involved in the processing, as well as the consequences it entails for data subjects, activities captured by Article 7 DSA may qualify as decisions based solely on automated processing, including profiling, that are prohibited under Article 22(1) GDPR. On the one hand, it is possible that some decisions by intermediary service providers to remove allegedly illegal content could significantly affect recipients of the service whose content is removed, although, as noted in the Article 29 Data Protection Working Party Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, such decisions are not within the scope of Article 22(1) GDPR unless the effect of the decision is similar to a legal effect. On the other hand, it is particularly important to assess the degree of human involvement in a system involving automated processing of personal data for the detection and removal of illegal content: if there is no human involvement, if human involvement is not meaningful, or if the human 'draws strongly' on the algorithmic recommendation generated by the system when deciding whether to remove the content, the decision would still be considered as being based solely on automated processing under Article 22(1) GDPR* […]."

- **Processing activities involved by the notice and action mechanisms** (Section 2.2.1)

8. The Guidelines should acknowledge that non-anonymous reporting is the default approach for notice and action mechanisms to ensure that providers can effectively respond to reports of illegal content, in line with the principle of data minimisation. The DSA provisions, including Article 16(2)(c) and recitals, make clear that the DSA generally requires identification of the notifier, while anonymous reporting must be allowed in certain limited cases, namely to report CSAM material.

9. In addition to cases where the identity of the person submitting a notice might be necessary for the provider to determine whether the relevant information constitutes illegal content as alleged (Recital 50 DSA), providers need to maintain a channel of communication to inform the notifier of their decision as to whether or not to act upon the notice, as set out in Recital 52 DSA. Further, providers need flexibility to verify a notifier's identity where reasonably necessary for the purpose of preventing misuse of the notice and action mechanism. To this point, Recital 53 DSA provides that "*notice and action mechanisms should allow for the submission of notices which are* ***sufficiently precise and adequately substantiated*** *to* ***enable the provider of hosting services concerned to take an informed and diligent decision***".[2] The last sentence of Recital 53 further states that "[e]*xcept for the submission of* [CSAM] *notices …* ***those mechanisms should ask the individual or the entity submitting a notice to disclose its identity in order to avoid misuse***". This makes it

[1] Article 29 Working Party Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01), p. 21.

[2] Emphasis added.

clear that allowing anonymous notifications creates a risk of misuse of these mechanisms, while Recital 63 DSA further emphasises that misuse of notification and action mechanisms may be prejudicial to the *"fundamental rights and freedoms* [of individuals] *as enshrined in the Charter* [of Fundamental Rights of the EU]*, in particular the freedom of expression*".

10. To reflect the above, we respectfully suggest that the EDPB revise paragraph 30 of the Guidelines as follows:

> *"*[…] *In this respect, the EDPB would recall that personal data should be limited to those necessary for the specific purposes referred to in the DSA relevant provisions. Hence, for example, providers should generally not ask for notifiers' additional personal data than those referred to in Article 16(2) DSA. This considering that, when additional identification data are deemed to be necessary, the DSA expressly mentions them and that, according to Recital 50 the "notification mechanism should allow, but not require the identification" of the notifier, unless it ~~is~~ "might be necessary to determine whether the information in question constitutes illegal content". In addition, providers should determine when identification is reasonably necessary to prevent misuse of the notice and action mechanism, as set out in Recital 53. Therefore, the providers should enable the identification of the notifier, but should not make the submission of a notice contingent on their identity being provided (except where this is reasonably necessary to prevent misuse or where it would not be possible to determine otherwise the illegal content)."*

- **ADM in advertising and profiling** (Section 2.4.2)

11. As set out above, whether certain forms of targeted advertisements qualify as ADM is only subject to the GDPR. Further interpretation on the subject of ADM is not necessary, in particular not in the context of advertising transparency pursuant to Article 26(1) DSA, which makes no reference to ADM.

12. If the EDPB nonetheless considers it necessary to address ADM in the context of the DSA, the EDPB should follow the approach taken in the WP29 ADM Guidelines and clarify that behavioural advertisements and algorithmic recommendations do not typically result in a significant effect for the purpose of Article 22 GDPR, as they fail to rise to the required "*threshold for significance, which must be similar to that of a decision producing a legal effect*." Furthermore, the WP29 ADM Guidelines state that, while it is "*possible*" that targeted advertising may have a significant impact on individuals when considering the characteristics above, "*in many typical cases, targeted advertising would not have a significant impact on individuals*".

13. In this case, we suggest that the Guidelines clarify in paragraph 62 that personalised advertising does not typically fall within the scope of Article 22 GDPR:

> "[…] *To assess whether an automated decision to present a specific advertisement to an individual produces legal effects or similarly significantly affects him or her, several (non-exhaustive) characteristics of the personal data processing activity (including at the level of each individual advertisement delivery) should be taken into account, including the intrusiveness of the profiling process, the tracking of individuals across different websites, devices and services; the expectations and wishes of the individuals concerned; the way the advert is delivered; or using knowledge of the vulnerabilities of the data subjects targeted. However, in many typical cases, the decision to present targeted advertising based on profiling will not have a similarly significant effect on individuals*."

- **Recommender system opt-out** (Section 2.5)

14. A requirement that VLOPs and VLOSEs present profiling and non-profiling recommender system options equally, and a prohibition of the use of profiling recommender systems before selection by a recipient of the service, is not supported by the text of the DSA, and would impose rigid design obligations that go beyond the DSA's objective of ensuring transparency and user control, effectively standardizing how platforms must present and sequence recommender system options. Such prescriptive requirements risk undermining innovation in interface design and content curation, which are core elements of service differentiation and user engagement strategies. They would also likely contribute to "choice fatigue," as users are already faced

with multiple layers of consent and configuration decisions under existing regulatory frameworks, including the GDPR and the DSA's own transparency and control provisions.

15. In light of the above, we would respectfully recommend revising paragraph 87 to omit this text as follows:

> "*The EDPB welcomes [the opt-out] provision and recalls that, in providing different options for recommender systems to users, providers of online platforms should respect the principle of data minimisation and the requirements of data protection by design and by default under Article 5(1)(c) and Article 25 GDPR.* ~~*Therefore, providers of 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. Providers of VLOPs and VLOSEs may only use a recommender system based on profiling after the recipient of the service has chosen this option.*~~"

- **Risk assessments and DPIA requirements** (Section 2.7)

16. The Guidelines should clarify that a data protection impact assessment (**DPIA**) is only required if the GDPR's threshold is met, even in the context of the DSA's Article 34 risk assessments. The concept of systemic risk to the protection of personal data in the DSA is not identical to the threshold for a DPIA set out in Article 35 GDPR. Systemic risks refer to widespread or structural risks at the platform level, which may affect large groups of users, but these do not necessarily cause a high risk for individuals, which is the threshold under Article 35 GDPR. In contrast, a high risk under Article 35 GDPR is about specific processing operations that are likely to have a significant impact on the rights and freedoms of individuals. We recommend the Guidelines confirm that a DPIA is only required if the systemic risk relates to processing personal data which meets the GDPR's criteria of high risk for individuals.

17. To clarify this, we respectfully recommend revising paragraph 99 as follows:

> *"*[…] *Potential ways of tackling such possible risks include appropriate implementation of data protection by design and by default under Article 25 GDPR and the adoption of mitigating measures in Article 35(1)(d) DSA. In the case of a systemic risk affecting the fundamental right to the protection of personal data, that is additionally not limited to individual users* *and is likely to result in a high risk to the individuals' rights and freedoms*, *a data protection impact assessment (DPIA) pursuant to Article 35 GDPR will likely be mandatory. In any case, it should be assessed whether the processing fulfils two or more of the criteria from the Article 29 Data Protection Working Party Guidelines on DPIA and, in some cases, a data controller can consider that a processing meeting only one of these criteria requires a DPIA. In addition, it should be noted that the GDPR requires the processing of personal data in accordance with lawfulness, fairness and transparency and free from discrimination, in particular with Articles 5, 22, 24 and 25 as well as Recitals 71 and 75 GDPR."*