AIAL's Comments to the EDPB Consultation for Guidelines 3/2025 on the interplay between the DSA and the GDPR (Version 1.1)

Date: 31st October 2025

Cite as: Harshvardhan J. Pandit (2025, October) "*AIAL's Comments to the EDPB Consultation for Guidelines 3/2025 on the interplay between the DSA and the GDPR Version 1.1*" AI Accountability Lab (AIAL). https://aial.ie/research/policy/consultation-2025-EDPB-Guidelines-3-2025-DSA-GDPR
DOI: 10.5281/zenodo.17496778

ABOUT AIAL

The AI Accountability Lab (AIAL) is a dedicated research lab within Trinity College Dublin that is focused on ensuring that the wider AI ecology — from research and product development, to regulation — centres public interest, particularly, the most marginalised and disenfranchised in society. Our inquiries into AI accountability, therefore, span from studies of large systems, structures, and ecologies (such as the AI field itself and regulatory processes) to executions of audits and evaluations on specific AI models, tools, and training datasets. We recognize that AI accountability research is most impactful when it can inform the public, impacted groups, and policy makers. Thus, we aim for active policy translation of our (as well as field wide) research.

You can find more information about the AIAL on its website at https://aial.ie/.

AUTHOR BIO

Dr. Harshvardhan Pandit is a Research Fellow in the AI Accountability Lab in Trinity College Dublin. His research interests are focused on solving real-world challenges associated with privacy, legal and regulatory compliance. Dr. Pandit is a nominated technical expert by the European Data Protection Board (EDPB). Dr. Pandit is also a member of the National Standards Authority of Ireland (NSAI), and through it participates within CEN/CENELEC and ISO groups on cybersecurity, privacy, and artificial intelligence, and is the co-editor for the ongoing ISO/IEC 27560 PII Processing Records standard. Additionally, Dr. Pandit also engages with standardisation activities in IEEE, in particular regarding P7012 machine-readable privacy terms, and in W3C as the chair of the W3C Data Privacy Vocabularies and Controls Community Group (DPVCG) that develops interoperable vocabularies for privacy and data protection activities based on legal and practical requirements.

This document represents the answers prepared by the team at AI Accountability Lab (AIAL) for the European Data Protection Board's (EDPB) public consultation for the *Guidelines 3/2025 on the interplay between the DSA and the GDPR Version 1.1*[1]. The consultation was open from 12th September until 31st October 2025, during which the AIAL team submitted its response.

Feedback

For the rest of the document, the content from the EDPB guidelines that we are providing comments on are provided in a box with blue text along with the relevant Point number through which they can be identified. Emphasis has been added only for the purposes for signalling the context of our response, which follows after the box in normal black text.

> 2. Intermediary service providers typically **qualify as controllers or processors** under the GDPR if they process personal data, depending on whether they determine the purposes and means of the processing (thereby qualifying as controllers) or merely process data on behalf and under the instructions of the controller (thereby qualifying as processors).

We request the EDPB guidelines to also reference the concept of '*third party*', who under the direct authority of the controller or processor, are authorised to process personal data.[2] While the 'third party' may have its own role as a controller within its own perspective, the association of an intermediary service as a third party is relevant to distinguish cases where the relationship of the intermediary service provider is outside the context of an existing relationship between a controller, processor, and data subject.[3] For an example in the context of the DSA, this can be an intermediary service provider that also collects data from other controllers through methods such as tracking and profiling of the users, and in this way also act as third parties for the data subjects for whom they are controllers.

For an example in the context of the GDPR, consider that a cloud hosting provider provides storage and retrieval of personal data, and is thus an intermediary service provider under the DSA.[4] If the cloud provider sells its services directly to the data subject, it likely acts as the controller. If the cloud provider is instead engaged by another service provider as part of its services provided to the data subject, then the

[1] https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2025/guidelines-32025-interplay-between-dsa-and-gdpr_en
[2] Article 4(10) GDPR
[3] Section 5 EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR
[4] Article 3(g)(iii) DSA

cloud provider likely acts as a processor. These are consistent with the points mentioned in the current EDPB guidelines. Now consider the situation where an entity acting as a controller sends data to the cloud provider for storage, such as when the data subject uses their service and the collected personal data is stored in the cloud. The cloud provider, in addition to acting as a processor for storing personal data, also scans the stored data to identify specific individuals of interest through means such as fingerprinting or facial recognition. In such cases, the cloud provider acts both as a processor and as a third party, and it is not sufficient for the data subject to only be informed about such recipients as processors. This is in line with the accepted meaning of recipients under the GDPR.[5]

> 14. … Insofar as possible, these actions should not involve **any processing** of personal data.

If the data regarding illegal content being analysed is personal data, such as when it also includes assessing who posted it, when, where, etc. – then it is inevitable that the processing also involves personal data by virtue of the analysis involving this information. Point 14 of the EDPB guidelines should therefore be amended to state: … *where the data being analysed itself constitutes as personal data as per Article 4(1) of the GDPR, for example because it contains identifiable information about an individual or it is information related to an individual, then insofar as possible, these actions (1) should not involve processing of any additional personal data solely for such purposes; and (2) should engage sufficient technical safeguards such as pseudonymisation.*

> 21. … Furthermore, processing that relies on Article 6(1)(c) GDPR must be **proportionate to the legitimate objective pursued**, meaning that there must be no other less intrusive means which, at the same time, would be as effective to pursue the objective. …

The guidelines should provide clarification that GDPR Article 4(1)(c) legal obligation as a legal basis can only be invoked if the 'necessity' principle is also satisfied under GDPR.[6] This follows from the phrasing of the legal basis, which states "processing is **necessary** for compliance with a legal obligation" (emphasis added). As the principles

[5] Article 4(9) GDPR
[6] Legal Bases for Processing Personal Data December (2019), Guidelines published by the Irish Data Protection Commission https://www.dataprotection.ie/sites/default/files/uploads/2020-04/Guidance%20on%20Legal%20Bases.pdf

of necessity and proportionality are related but have distinct implications in EU law,[7] the guidelines should mention both of them in a manner similar to the explanation of legitimate interests in Point 18.

> 22. … If Article 22(1) GDPR is applicable, intermediary service providers need to verify whether **an exception to the prohibition** applies under Article 22(2) GDPR, notably whether the processing is authorised by EU or Member State law that fulfils the requirements of Article 22(2)(b) GDPR …

The guidelines should also clarify the application of Article 22(2)(c) GDPR which allows the use of explicit consent of the data subject as an exception to the use of automated decision making described in Article 22(1). The notion of 'explicit consent' should be explained in accordance with and as a reference for 'EDPB Guidelines 05/2020 on consent under Regulation 2016/679'. The validity of 'explicit consent' should be described as requiring the data subject to explicitly and solely give their affirmative consent regarding the automated decision making. Other forms of consent, or inclusion of these in the terms for the platform, would not be considered as valid forms of explicit consent. Additionally, the explicit consent must be obtained with "*meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing*" as required by GDPR Article 13(2)(f) and Article 14(2)(g). This necessitates information about the mechanism used in automated decision making (i.e. logic),[8] the personal data categories being processed to derive the decision,[9] as well as the effect of the decision on the data subject.[10] This is also relevant to the transparency principle mentioned in Point 23.

Where the effects of automated decision making constitute as "legal effects" within the meaning of Article 22(1) GDPR, the data subject has the right to object to such uses if the decision making was without meaningful human intervention (as mentioned in Point 22). The guidelines should explicitly mention this right of the data subject and its invocation in relation to the DSA's obligations. In particular, the right to object to

[7] Necessity & Proportionality (2025) European Data Protection Supervisor https://www.edps.europa.eu/data-protection/our-work/subjects/necessity-proportionality_en

[8] We note here that generic language referring to "AI" or "algorithms" cannot satisfy this requirement, nor can statements such as "use of sophisticated algorithm xyz" as the data subject cannot be expected to understand the existence or the use of such technologies.

[9] Though Article 13 states information to be provided when personal data are collected, the understanding of 'logic' in automated decision making cannot be complete without information on which categories of personal data are being utilised. This can be understood from the general principle of an algorithm not being completely defined without the inputs it will require.

[10] Effect refers to the consequence of the decision on the data subject, and includes aspects such as revocation of account or features, termination of contract, change in data subject' ability to use the service. The GDPR requires that such effects be especially noted when they constitute "legal effects" as mentioned in Article 22(1).

automated decision making under the GDPR must be interpreted as being necessary to be provided regardless of the application of the DSA. This means intermediary services that perform decision making solely via automated means and without meaningful human intervention, as is described in Point 22, must also enable the data subjects to challenge this decision through the right to object described in GDPR Article 22(1).

24. Lastly, in accordance with the EDPB Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk", voluntary or mandatory actions triggered by intermediary service providers under Article 7 DSA are likely to fulfil several criteria that would indicate that **carrying out of a DPIA shall be required**. Such criteria include evaluation or scoring, automated-decision making with legal or similar significant effects and systematic monitoring. Providers of VLOPs are also likely to fulfil the large-scale processing criterion.46 Under Article 36 GDPR, intermediary service providers may also need to consult the supervisory authority prior to processing where a data protection impact assessment under Article 35 GDPR indicates that the processing would result in a high risk in the absence of measures taken by the intermediary service provider to mitigate the risk.

The necessity and requirement for a DPIA is defined in Article 35(1) of the GDPR, and in addition is also defined for each Member State due to the mechanism established in Article 35(4) of the GDPR. Our analysis of Member State's DPIA required activities show variance in the conditions and criteria.[11] While criteria such as evaluation, scoring, monitoring, and decision-making have a well established basis through the application of the GDPR, other criteria such as "use of AI" or "processing resulting in access or exclusion to services" have a fragmented applicability only in specific jurisdictions. We therefore urge the EDPB to harmonise the DPIA required processing activities across Member States to provide a consistent harmonised application of the GDPR.

We also point to the fragmentation in DPIA required conditions as being of significance to the overlap between the GDPR and the DSA. Some DPIA required criteria are only present within specific jurisdictions, but are relevant to the operations of an intermediary service provider in accordance with the DSA, in particular regarding the obligations under Article 7. For example, an intermediary service provider is operating from Ireland and is also serving data subjects in Italy. The Garante (Italian DPA) considers "*exclusion to service*" as a sufficient criteria to require a DPIA whereas the Irish DPC does not.[12] This means the same intermediary service provider has a different

[11] Impact Assessment Requirements in the GDPR vs the AI Act: Overlaps, Divergence, and Implications (2025) Tytti Rintamäki, Delaram Golpayegani, Dave Lewis, Edoardo Celeste, and Harshvardhan J. Pandit https://doi.org/10.31219/osf.io/6qhzj
[12] See Footnote 10 for regarding variance in DPIA required criteria across Member States

notion of risk to the data subject for the same processing activities based on where they are operating from, and this also affects their assessment obligations under the DSA as a consequence of potentially not having to conduct a DPIA.

> 30. … This considering that, when additional identification data are deemed to be necessary, the DSA expressly mentions them55 and that, according to Recital 50 the ”notification mechanism should allow, but not require the identification” of the notifier, unless it is “necessary to determine whether the information in question constitutes illegal content”. 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 it would not be possible to determine otherwise the illegal content).

We appreciate the clarity and explicitness of the EDPB's statements regarding the limitation of DSA's identification obligation regarding notifiers. We request the EDPB add an additional explicit statement that asserts that the providers should not necessitate the creation of an account or any other registration or similar mechanism as the means to achieve identification. Such clarification would be helpful for providers to understand that the notification mechanism is envisaged as separate to the provider's own services, and being part of that service is not a precursor for the reporting by the notifier. This is evident in the DSA Article 16(1) which uses the phrase "*any individual*" when referring to notifiers. Under GDPR, the requirement for an account would thus qualify as collecting and processing more personal data than that which is necessary for the purpose (or notification). By extension, the requirement for an account when the notifier does not have one would also violate the GDPR's data minimisation principle.

We also request the EDPB to clarify that the DSA's obligations regarding the identification of the notifier do not create an absolute notion of identity of the notifier i.e. the provider does not have to establish the identity of the notifier beyond that which is necessary to fulfil the purposes of notification as required by the DGA. Therefore, additional statements clarifying, ideally with an example, of the provider requesting ID documents, selfies, or other forms of "proof" to establish identity will likely constitute excessive personal data unless the provider can establish that this is necessary for the reporting of illegal content. An example in this context that allows the use of identity could be based on the reporting of deep fakes of an individual, where the notifier is the individual themselves, and thus can establish their identity as being necessary to help the provider remove the reported deep fake content. A similar example where identity is not necessary could be the reporting of violent speech that does not necessitate establishing the identity of the notifier through uploading an ID

document or similar mechanism. These will also help clarify the interpretation of GDPR in a concrete manner and assist the relevant authorities and notifiers in utilising the DSA's provisions with certainty regarding the protections provided by the GDPR.

We also request the EDPB guidelines to clarify the further use of personal data collected to fulfil the DSA's notification obligations, particularly in terms of using this data to conduct operations such as abuse detection, security measures, and fraud prevention. The legal bases for such measures should be separate from the legal obligation to fulfil the DSA obligations, and it is likely that that provider must rely on legitimate interests as the legal basis under GDPR to conduct these. As has been explained in earlier Points, the use of legitimate interest in this manner cannot justify collection of additional personal data than what is relevant in the fulfilment of the legal obligation and must additionally also fulfil the assessment of necessity and proportionality before using legitimate interests. This is already described to a certain extent in Points 41 and 42, but it is pertinent to also provide this guidance or a link to this application within the guidelines.

> 42. … It is also important that online platform providers are transparent towards data subjects in rela- tion to processing they may carry out within the remit of Article 23 DSA and provide them with all elements of information required under Articles 13 and 14 GDPR, in line with the conditions set forth in Article 12 GDPR. …

We request the EDPB to clarify in the guidelines the following aspects regarding the requirements established in GDPR Article 13(2)(f) regarding information to be provided regarding automated decision making:

1. The statement in the GDPR Article 13 regarding "meaningful information about the logic involved" requires that the data subjects must explicitly be provided information about how the decision was made following the notification with sufficient description of the automated process;
2. The statement in GDPR Article 13 regarding "*as well as the significance and the envisaged consequences of such processing for the data subject*" necessitates a prior provision of information to the data subject that the use of automated decision making will result in a suspension of their account.
3. Following from (1) and (2) above, it is also necessary to inform the data subject if the suspension of their account will prevent or otherwise affect their ability to exercise *any* relevant right, including those provided by the GDPR.
4. Where the suspension of an account affects the ability of the data subject to engage the service, which they access under a contract, then such suspensions must be considered as "legally significant effects" as they constitute a challenge

to the data subject's use of the service under a contractual relationship which has a binding effect in contract law regarding the obligation of the service provider to provide said service to the data subject.

5. Where the suspension of an account affects the ability of the data subject to exercise or in any way access or utilise a right, then such suspensions must also be considered as "legally significant effects" as bearing a direct impact on the data subject's rights.

From the above, it is obvious that the affected processing to fulfil the DSA's obligations requires a corresponding data protection impact assessment under GDPR Article 35(1) as it poses a high risk to the data subject's rights and freedoms. This means the service provider must be equipped, before the processing can be initiated, to identify issues such as errors, "bugs", or any other defects in the process of suspension, and must have sufficient measures in place to remedy them. This is an essential aspect of the GDPR's obligations to prevent unfair termination or otherwise reduction in the service for data subjects unless it has been justified by a corresponding processing under the DSA's notification mechanism.

We also request the EDPB to explicitly note that a suspension of accounts under the DSA does not discount or otherwise free the service provider under their obligations to exercise any of the GDPR rights, in particular the ability of the data subject to withdraw consent (Article 7), object to legitimate interests (Article 21), or access information (Article 15). The data subject also has the right to not be subjected to decision making solely based on automated decision making (Article 22). From these, it is clear that a suspension of accounts under the DSA should not in any way affect the ability of the data subject to exercise *any* of their GDPR rights, and that where such suspensions are done using automated decision making, the GDPR provides the data subject with the right to a human review (Article 22(3)). Providing this information in the guidelines will assist in clarity regarding the practices which service providers should not engage in, and to guide them towards a responsible continuation of the data subject's rights – in particular those under Article 22(3). While some of this is later covered in Point 42, the information regarding the full application of Article 22 should include the obligation regarding human intervention.

> 43. Article 25(1) DSA obliges providers of online platforms to design, organise, and operate their online interfaces in a way that does not impair the ability of recipients of the service to make autonomous and informed decisions. …
>
> 44. Data protection authorities are responsible for addressing deceptive design patterns if they are covered by the GDPR, which needs to be assessed on a case-by-case basis. …

We request the EDPB to consider an expanded scope in its description of "deceptive design patterns" by also considering the use of such malpractices in contexts relevant to the exercising of rights. For example,

- The use of design to hide information, or in any way influence the data subject into making decisions such as accepting the service by portraying it as being privacy friendly when it is not, or by hiding risks which must be informed, or by making it difficult for the data subject to access information through obfuscation, sheer length or number of links that are excessive to navigate, or other forms which form 'dark patterns'.
- As above, by making it difficult to impossible for the user to engage with the service provider to obtain this information, or not providing complete information, or adding unreasonable or unjustified delays. These and other similar tactics should also be considered as design patterns when they are implemented through the UI/UX in a systematic manner and have the effect of denying necessary information required for the exercise of rights.
- By asking for confirmation where it is not necessary, or otherwise adding additional steps for the data subject to exercise their rights. For example, regarding the right to access under Article 15 or to object to legitimate interests under Article 21, the data subject being asked to provide excessive information or to navigate a complex interface solely to submit their request.
- By requiring users to log in before they are able to exercise rights for cases where they are not the users of the service: For example, Instagram[13] significantly degrades the experience of exercising rights by not providing information on this link provided in its terms, and instead requires the user to navigate to a series of pages which ultimately do not provide information on exercising the rights (e.g. Article 15 access to information and Article 21 objecting to legitimate interests). The users only recourse is to manually draft a complaint which is then ignored seemingly automatically by their systems.

[13] https://www.instagram.com/help/support/privacy/

- By asking the data subject to justify their exercise of rights: for example, Instagram requires the user to provide a statement explaining why they feel the objection is needed, and which Meta then uses to ignore the objection. This is despite the fact that the GDPR's Article 21(1) uses the phrase "*unless the controller demonstrates compelling legitimate grounds*" and does not require the data subject to justify their objection unless this is necessary.[14]

Since in each of these cases, there is a significant use of UI/UX as the means to create friction, delays, and otherwise to frustrate the user into not being able to exercise their rights and thus their *free and informed decisions*, these should also be considered as deceptive design patterns in the meaning of Article 25 of the DSA.

~ END ~

[14] Point 71 Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR