Response to the EDPB public consultation on Guidelines 3/2025 on the interplay between the DSA and the GDPR

The undersigned associations have taken note of the European Data Protection Board's (EDPB) draft "Guidelines 3/2025 on the interplay between the DSA and the GDPR" (DSA-GDPR Guidelines), which have been circulated for public consultation until 31st October, 2025. We are grateful for the opportunity to provide comments on the draft Guidelines.

Executive summary

We welcome the public consultation organised by the EDPB in relation to its Guidelines 3/2025 on the interplay between the Digital Services Act (**DSA**) and the General Data Protection Regulation (**GDPR**), and appreciate the opportunity to comment on these **DSA-GDPR Guidelines**.

Clear guidance on the interaction between the DSA and the GDPR is essential, given the significance of both frameworks. Although the DSA-GDPR Guidelines represent a valuable step, they require further clarification and development in order to reduce legal uncertainty and ensure that key aspects of the DSA's application alongside the GDPR are adequately covered.

Areas of concern

- The DSA-GDPR Guidelines highlight consequences of the possible application of Article 22(1) of the GDPR in certain scenarios, but the vague examples make it such that it is unclear which processing activities would actually fall within the scope of that provision and why they might be considered to have significant legal or similar effects on users (in particular in connection with personalised advertising);

- Although the Guidelines provide guidance on the legal grounds for processing operations that stem from compliance with various DSA provisions, they fail to make any suggestion regarding the processing that may occur under Article 26 of the DSA. The Guidelines also impose a stringent interpretation of the GDPR security obligations in connection with such processing;

- The EDPB's considerations in relation to the concept of special categories of data and its broad scope (in particular on the extent to which the controller's intent can influence such classification) could negatively affect certain processing operations, for instance in relation to brand safety;

- In the Helsinki statement, the EDPB recently affirmed its commitments to foster cross-regulatory cooperation with non-data protection regulators and to ensure real world effectiveness of its guidelines. We are therefore concerned that guidelines that are at the crossroads of two landmark legislations - the GDPR and the DSA - are being drafted without the involvement of the digital services coordinators (DSCs) through the EBDS and the EU Commission. This approach does not align with the draft DMA guidelines, developed with the EU Commission and the AI Act guidelines, drafted with the AI Office, nor with the EDPB's own statements in its draft guidance (para 9 and 188). We therefore recommend that the DSC board and the EU Commission take an active part in the drafting of the Guidelines, and respectfully ask the EDPB to refrain from interpreting substantive provisions of the DSA that fall outside its competence as the Board of Data Protection Authorities;

- While acknowledging the absence of explicit cooperation duties between Data Protection Authorities and Digital Services Coordinators in the legislation, the Guidelines fail to propose the formal mechanisms needed to avoid legal uncertainty, duplicative proceedings, and inconsistent enforcement.

- Finally, the guidelines are very long, legalistic and tend to create obligations that are neither in the GDPR, nor in the DSA. Overall they lack a practical approach to provide solutions for organisations having to comply with both texts. This posture is contrary to the commitments made by the EDPB in the Helsinki statement ("develop common practices, methods, tools and common actions review guidelines to ensure their real-world effectiveness").

We therefore urge the EDPB to amend its DSA-GDPR Guidelines to take into account these concerns and the suggestions hereunder.

1) Automated decision-making and its irrelevance for advertising

The DSA-GDPR Guidelines state in para. 62 that the provisions of Art. 26(1) DSA – requiring meaningful information about the *"main parameters used to determine the recipient to whom the advertisement is presented and, where applicable, about how to change those parameters"* – *"may, depending upon the particular characteristics of the case, relate to data processing practices that might fall within the scope of automated individual decision-making and profiling that fulfil the criteria of Article 22(1) GDPR"*.

This draws from the Article 29 Working Party's "Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679" of 3 October 2017 (as revised on 6 February 2018), endorsed by the EDPB on 25 May 2018, and which state:

> *"In many typical cases the decision to present targeted advertising based on profiling will not have a similarly significant effect on individuals, for example an advertisement for a mainstream online fashion outlet based on a simple demographic profile: 'women in the Brussels region aged between 25 and 35 who are likely to be interested in fashion and certain clothing items'.*
>
> *However it is possible that it may do, depending upon the particular characteristics of the case, including:*
> - *the intrusiveness of the profiling process, including 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.*
>
> *Processing that might have little impact on individuals generally may in fact have a significant effect for certain groups of society, such as minority groups or vulnerable adults. For example, someone known or likely to be in financial difficulties who is regularly targeted with adverts for high interest loans may sign up for these offers and potentially incur further debt."*[1]

The reasoning in these automated decision-making Guidelines (hereinafter the **WP29 ADM Guidelines**) is simply referred to by way of a footnote in the DSA-GDPR Guidelines, but to date this reasoning has not been used or even tested in court. Unfortunately, it is so vague and unclear that even referring to it, without additional explanations, creates legal uncertainty. Moreover, this reasoning is not aligned with the risk classification of the AI Act, that classifies high risk AI as having an adverse impact on fundamental rights and does not include advertising or personalised advertising (see article 7 and Annex III).

[1] Article 29 Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 6 February 2018, WP251rev.01, p. 22.

The notion that the presenting of an advertisement to an individual – no matter how vulnerable – has legal effects on a data subject or "similarly significantly affects" the data subject is without support in law. First, profiling, whilst it may involve automated processing, is not itself a decision making process. Instead it is about evaluations, not decisions. It may form part of an eventual decision, but in itself profiling for advertising purposes cannot be considered to reach the threshold of automated decision making as described by the GDPR. Second, while vulnerable individuals may in certain circumstances be more amenable to persuasion, an advertisement is solely an invitation to seek out a brand, service or product. The advertisement itself does not change the legal situation of the viewer, nor does it make any further action inevitable. If a data subject sees an advertisement for something that they find desirable or that satisfies a particular need, the advertisement can at most be an initiator or factor in the data subject's thought-process. The EDPB also wrongly assumes that the actor presenting the advertisement would be aware of the vulnerability of the data subject. This overlooks the fact that as per the GDPR data minimisation principle, many ad tech providers only process pseudonymised data and do not profile individuals on the basis of their vulnerability. The prohibition of the DSA to profile individuals on the basis of special categories of data renders the potential inference of vulnerabilities even more complicated.

Advertisements need to be differentiated from many other situations that may have a legal or substantially equivalent effect on data subjects:

- Credit scoring in which the outcome affects the possibility for a data subject to benefit from a financial product, or situations in which an insurance contract's terms (such as the premium)
- Relying on ADM to deny someone access to an employment opportunity or a service agreement
- Relying on ADM to decide whether an individual can be admitted to a particular university or school

Therefore, reliance on unproven, outdated and potentially misinformed parts of the WP29 ADM Guidelines may give rise to difficulties for the DSA-GDPR Guidelines and may bring into question their foundations. In addition these guidelines date back to 2018 and have never been updated to take into account technological evolution and practices, including Privacy Enhancing Technologies.

We therefore request that they be amended to clarify that the selection and presenting of advertising <u>does not</u> fall within the scope of Article 22(1) GDPR. In particular, paragraph 62 should be reviewed to exclude the application of Article 22(1) GDPR to advertising, even personalised advertising, or should at least set out the specific and exceptional circumstances in which such provision would apply according to the EDPB (for instance based the AI Act's classification that targeted job ads falls under the high-risk category of the AI Act - or other laws).

2) Legal ground explanations regarding Article 26(1) DSA and security obligations

Article 26(1) DSA requires the provision of meaningful information about the *"main parameters used to determine the recipient to whom the advertisement is presented"* as well as "*the natural or legal person on whose behalf the advertisement is presented*" and "*the natural or legal person who paid for the advertisement if that person is different from the natural or legal person referred to in point (b)*".

In the Open Web, providers of online platforms generally rely on third-party companies for selling ad placement on their services. Such companies may as a result have to transmit and/or facilitate the rendering of the ad-level information required under Article 26(1) DSA, which may involve the processing of personal data as correctly pointed out by the DSA-GDPR Guidelines.

As Article 26(1) DSA only imposes a direct obligation on providers of online platforms, this creates a two-tiered approach in terms of legal grounds that should be reflected in the DSA-GDPR Guidelines.

To the extent that the presenting of the ad-level information required by Article 26(1) involves the processing of personal data from the perspective of online platforms, the DSA-GDPR Guidelines should make clear that legal obligation may be an appropriate legal ground. This would be aligned with the rest of the Guidelines which appropriately recognise reliance on the legal obligation legal basis for processing of personal data that stems from compliance with DSA provisions.

In practice, extending the possibility to rely on the legal obligation to third-party entities that support or cooperate with online platforms in meeting their DSA obligations would enhance consistency and legal certainty across the digital advertising supply chain. These entities often operate under contractual or technical arrangements that are directly connected to the platform's compliance with Article 26(1). Enabling them to rely on the same legal ground would therefore reduce unnecessary complexity and ensure more coherent compliance approaches where processing serves the same regulatory purpose. In addition, there may be situations where these entities act as processors on behalf of online platforms, specifically or including for the processing underlying compliance with Article 26(1), in which case the legal basis relied upon will necessarily be the one of the online platform.

Alternatively, where third-party companies cannot rely on the legal obligation legal basis, the DSA-GDPR Guidelines should make clear that legitimate interest may be an appropriate legal ground. A legitimate interest assessment could also be recognised by the EDPB as being straightforward for the purposes of Article 26(1) compliance:

- The legitimacy of the interest is self-evident, as a result of lawfulness of the processing to enable compliance with Article 26(1). While that interest is the interest of a third party

in this specific case (as the entity in question is not the online platform subject to the legal obligation), that interest is easily defined and lawful. Additionally, the processing is intended at providing additional and meaningful information to end-users about the advertisements they see online.

- The necessity test would also be easily fulfilled, as the processing would relate to the transmission or rendering of the information referred to in Article 26(1). Without such information, the interest (enabling compliance with Article 26(1)) could not be achieved.

- The balancing test would also be achievable, notably already by virtue of the reasoning behind Article 26(1). It is worth stressing in this respect that while a data subject must have the possibility to object to the processing of personal data[2], in this particular case it would be necessary to recognise that statutory compliance by the provider of the online platform with Article 26(1) and the objective of that provision would render any objection self-defeating. Therefore, for the purposes notably of the balancing test, it would be important for the EDPB to recognise that, for any company along the chain in whose respect the processing of information to facilitate compliance with Article 26(1), there are *"compelling legitimate grounds"* for the processing that *"override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims"*, in accordance with Article 21(1) GDPR.

In this context, paragraphs 51 to 56 should be amended to reflect these considerations, in order to provide greater legal certainty as to the legal grounds that can be relied upon specifically for compliance (by providers of online platforms) or to enable compliance (from the perspective of third-party companies) with Article 26(1).

While paragraph 78 rightly emphasises the need for appropriate technical and organisational measures and compliance with GDPR principles for the processing that may be required by third-party companies to facilitate online platform's compliance with Article 26(1), it overstates the restrictions to third-party companies' access to personal data by stating that "*Compliance with the transparency obligations set out in Article 26 DSA should not entail further sharing of personal data with intermediaries.*"

The GDPR does not categorically prohibit access to personal data; rather, it requires that any processing have a valid legal basis, adhere to the principles of purpose limitation and data minimisation under Article 5 GDPR, and respect the safeguards of Articles 25 and 32 GDPR.
Access to data is permissible provided it is necessary for the - purposes for which the processing is carried out and provided that this data processing is not repurposed for unrelated activities without a valid legal basis. In other words, so long as third-party companies process data in line with the purpose of facilitating online platform's compliance with Article 26(1) and implement robust safeguards, access to relevant personal data, including personal data they did not already hold as part of their other processing activities, is compatible with the GDPR.

[2] Article 21(1) GDPR.

Accordingly, paragraph 78 should be reviewed by adapting the sentence that cautions against further sharing of personal data in the context of compliance with the transparency obligations set out in Article 26 DSA and replacing it with a reminder of the need to consider data minimisation and purpose limitation in the context of assessing compliance with the GDPR.

3) Special categories of data and limits to the broad scope thereof

The DSA-GDPR Guidelines refer to Article 9 of the GDPR in several instances, notably to highlight the prohibition under Article 26(3) DSA for providers of online platforms to present advertisements to recipients of the service *"based on profiling […] using special categories of personal data"*.

These special categories of personal data are defined by Article 9(1) GDPR as personal data *"revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation"*.

Recent CJEU case law has suggested that the scope of Article 9(1) GDPR can be very broad:

- In the *Lindenapotheke* case, the CJEU considered that when a customer of an online pharmacy enters information for the ordering of "over-the-counter" pharmacy-only medicinal products, this information constitutes "data concerning health" within the meaning of Article 9(1) GDPR, *"even where it is only with a certain degree of probability, and not with absolute certainty, that those medicinal products are intended for those customers"*[3].

  In other words, the word "revealing" within the definition of special categories of data does not require certainty but a certain degree of probability.

- In the *Bundeskartellamt* case, the CJEU stressed that Article 9(1) GDPR covers scenarios also where the information in question is incorrect (i.e. does not reveal accurate information about the categories of data in question) but also that the rule of prohibition to process such categories of personal data applies irrespective of *"whether the controller is acting with the aim of obtaining information that falls within one of the special categories"*[4].

  Put differently, even an incidental and unintentional receipt of special categories of data leads to the application of the processing obligation.

[3] CJEU, *Lindenapotheke*, 4 October 2024, C-21/23, EU:C:2024:846, para. 90.
[4] CJEU, *Bundeskartellamt*, 4 July 2023, C-252/21, EU:C:2023:537, para. 70.

- In the *OT v Vyriausioji tarnybinės etikos komisija* case, the CJEU held that the publication of a spouse's name could in and of itself indirectly reveal sexual orientation and that Article 9(1) GDPR applied: *"the publication, on the website of the public authority responsible for collecting and checking the content of declarations of private interests, of personal data that are liable to disclose indirectly the sexual orientation of a natural person constitutes processing of special categories of personal data"*[5].

  The actual intent of the controller was not taken into account in this context: just the act of making information available about a spouse was deemed to be *"liable to disclose indirectly the sexual orientation"* of the data subject.

In this context, as Article 9(1) GDPR grows in scope through case law, there is a general concern of abuse of Article 9(1) GDPR by authorities or data subjects keen to reinforce a subjective view of its scope. Although many companies operating in the sector (including companies not in scope of the DSA) already do not support the processing of special categories of data for personalised advertising, and such processing is prohibited by industry standards such as the Transparency and Consent Framework (TCF), an overly broad interpretation of the definition creates legal uncertainty and unnecessary complexity.

For example, a brand safety system may use contextual signals - such as the presence of keywords related to certain themes (e.g. political conflicts) to avoid placing a given advertisement from appearing alongside content relating to political issues. This processing is carried out solely for safeguarding the brand's reputation and not to infer or reveal any users' political opinions. Accordingly, it is critical for the EDPB to recognise that objective elements are key. There must be a demonstrable intention to reveal the special categories of data, and an actual inference by the controller.

Although the *Example 2* listed by the EDPB under paragraph 75 of the DSA-GDPR Guidelines already hints at this, highlighting the situation where a company *"uses inferred religious beliefs from geolocation […] to predict lifestyle and shopping patterns"*, a more explicit reference in paragraphs 72 to 76 to the need for inference in order to trigger Article 9(1) GDPR would be necessary as well as a more practical example.

4) Proportionality standard for age verification

The Guidelines' current interpretation of the necessity and proportionality standard applicable to age assurance under Article 28 sets a very high threshold that risks undermining effective implementation. Instead of considering in the abstract that online identification or retention of users' age or age range should generally be avoided, the Guidelines should align with the risk-based approach of the GDPR by recognising the need for differentiated solutions on a case-by-case basis to meet the objectives pursued under Article 28(1) and (2) DSA. This would

[5] CJEU, *OT v Vyriausioji tarnybinės etikos komisija*, 1 August 2022, C-184/20, EU:C:2022:601, para. 128.

more closely align with the Commission's Article 28 DSA Guidelines[6] which say that platforms should adjust access to features, content or activities based on the evolving capabilities of minors. This presupposes that the exact age of the minor is known; for example to offer an age-stratified experience. The draft Guidelines would appear to make this highly challenging to achieve.

The Guidelines should also acknowledge situations where age verification mechanisms may be required under other EU or national legal frameworks already applicable to DSA-regulated services, including consumer protection or child safety regulations, as well as the varying age thresholds across Member States.

5) Cooperation between regulators and consistent enforcement thereof

The Guidelines were not elaborated jointly with the European Board for Digital Services (EBDS), national Digital Services Coordinators (DSCs) or the EU Commission. This raises uncertainty regarding whether they adequately capture the perspectives of authorities that are effectively assigned with the responsibility for enforcing the DSA. We strongly recommend the EDPB to ensure meaningful consultation with the EBDS, national DSCs and the EU Commission to reflect their perspectives in the final Guidelines - in line with the Helsinki statement and with the EDPB's approach on their DMA and AI Act Guidelines.

The lack of coordination with DSCs is particularly problematic given the Guidelines include multiple instances where the EDPB interprets substantive provisions of the DSA beyond its mandate. This occurs for example in paragraphs 15 and 16 on the assessment of available technologies for detecting illegal content - that the EDPB considers high in relative and absolute numbers - as well as paragraphs 52, 67, 75, 76, 78, 86, 87, and in sections 2.3 and 2.7. In particular, section 2.3 of the Guidelines attempts to interpret Article 25 of the DSA, which addresses the use of dark patterns exclusively in relation to the processing of non-personal data, and therefore lies beyond the EDPB's remit. Moreover, the EDPB refers to a parliamentary resolution as a source of legal interpretation (paragraph 46, footnote 77) - a document which carries no binding legal effect and cannot serve as an authoritative source for interpreting EU legislation.

It should be for the DSCs or EBDS to make these types of assessments and for the EDPB to rely on this expert assessment. As a result, we recommend the EDPB to delete interpretations of DSA provisions it makes in its own capacity, and limit its guidance to clarifying the application of the GDPR where processing of personal data is at stake.

Additionally, while the Guidelines acknowledge in paragraphs 117 and 118 that neither the GDPR nor the DSA explicitly provides for a duty of cooperation, they do not address the

[6] See Communication from the Commission – Guidelines on measures to ensure a high level of privacy, safety and security for minors

practical implications of this gap. The absence of formalised consistency mechanisms risks creating significant legal uncertainty and exposes providers of online platforms and intermediary services to the possibility of duplicative proceedings and inconsistent enforcement by data protection authorities and DSA competent authorities. Such outcomes would not only undermine legal certainty but also run counter to the principles of proportionality and procedural fairness. To prevent these risks, we invite the EDPB to engage with the EBDS, DSCs and the European Commission in order to create a structured and formal framework for inter-regulatory consultation and coordination.

It is also essential to maintain a clear boundary between enforcement under the DSA and the GDPR. Recent actions by certain national data protection authorities, such as the Berlin DPA[7], raise concerns about attempts to use DSA mechanisms to pursue GDPR enforcement. Applying the DSA's notice-and-action framework - intended at facilitating the reporting of illegal content - to resolve complex data protection matters undermines the GDPR's dedicated procedures and safeguards. The distinct objectives and enforcement processes of each regulation must be respected, and the Guidelines should make clear that the DSA cannot serve as a shortcut for GDPR enforcement. The Guidelines should also clarify that the GDPR's One Stop Shop mechanism remains central for cross-border privacy issues, even when DSA regulators are engaged.

* * *

We thank you in advance for taking into consideration these concerns and suggested solutions and to ensure that this public consultation leads to meaningful changes to the Guidelines to that end.

[7] See https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2025/20250627-BlnBDI-Press-Release_DeepSeek.pdf

List of signatories

IAB Europe: IAB Europe is the European-level association for the digital marketing and advertising ecosystem. Through its membership of national IABs and media, technology and marketing companies, its mission is to lead political representation and promote industry collaboration to deliver frameworks, standards and industry programmes that enable business to thrive in the European market.

Alliance Digitale: The Digital Marketing and Data Association - Alliance Digitale is dedicated to representing all professions and professionals linked to data and digital marketing in France, with the aim of promoting their development and defending their interests. Alliance Digitale's mission is to represent the interests of all its 300 members, regardless of their size or position in the value chain. Alliance Digitale is a key contact for public authorities and regulators at both French and European level. The association is also an important partner for the media and other professional associations in the digital ecosystem. Alliance Digitale is the French representative of three emblematic international digital marketing and data networks: IAB, FEDMA and GDMA.

BVDW: The German Association for the Digital Economy (BVDW) is the advocacy group for companies that operate digital business models or whose value creation is based on the use of digital technologies. With its members from the entire digital economy, the BVDW is already shaping the future today through creative solutions and state-of-the-art technologies. As a catalyst, guide, and accelerator for digital business models, the association relies on fair and clear rules and advocates for innovation-friendly framework conditions. BVDW always keeps an eye on the economy, society, and the environment. In addition to DMEXCO, the leading trade fair for digital marketing and technologies, and the German Digital Award, the BVDW also organizes the CDR Award, the first award ceremony in the DACH region for digital sustainability and responsibility, as well as a variety of specialized events.

IAB Italia: IAB Italia is the Italian chapter of the Interactive Advertising Bureau, the leading association of digital marketing and advertising. Since 25 years it has significantly contributed to the diffusion of digital culture and to the acceleration of market growth in Italy through the development of ethical and sustainable communication. IAB Italia pursues its mission through the realisation of vertical events, special projects, training activities and with Intersections, the largest Italian event dedicated to marketing and digital innovation on the most relevant issues for the industry, involving top national and international speakers. The Association has more than two hundred members, among the main Italian and international operators active in the interactive advertising market.

IAB Polska: IAB Polska is a Polish advertising industry organisation that unites and represents entities of the interactive industry. IAB Poland members include more than 250 companies, including the biggest web portals, global media groups, interactive agencies, media houses and

technology providers. In 2012 the organisation received the MIXX Awards Europe, honouring the best IAB bureau in Europe.
The mission of IAB Poland is to support development of the Internet industry and take regulatory actions to enhance the competitiveness of the market, conducting research projects, leading educational programs and providing legal protection.

IAB Spain: IAB Spain undertakes a comprehensive mission as a forum for meeting and representing the digital advertising industry in Spain. Since its inception in 2001, IAB Spain has played a crucial role in the promotion and development of digital advertising. IAB Spain's mission unfolds on various strategic fronts: With the aim of contributing to the proper regulation of the sector, by contributing, assisting, and fostering conversations with public administrations. Furthermore, IAB Spain proactively works on creating industry standards, with the goal of establishing guidelines and best practices that promotes the sustainable and ethical growth of digital marketing, advertising and therefore promoting innovation and positivities for the society. Members of IAB Spain encompass a wide range of stakeholders in the digital advertising ecosystem, including digital and audiovisual publishers, platforms, media agencies, marketing and advertising agencies, advertisers, consulting firms, technology providers, advertising networks, and others, such as eCommerce and research institutes.

SPIR: For over 20 years, the Association for Internet Progress (SPIR) represents the most important players of the Czech Internet economy from among media publishers, media agencies and technology companies with an annual turnover of more than 37 billion Czech crowns (1,5 billion EUR). The services offered by SPIR members are used by over 90% of the population of the Czech Republic. Member companies pay 3 billion Czech crowns (120 million EUR) a year in taxes and other fees to the state budget and employ 7,500 people throughout the Czech Republic. SPIR operates the only official measurement of Czech Internet traffic NetMonitor, monitoring of Internet advertising AdMonitoring and provides expert analyses of the development of the Czech Internet market.