BCLP. Client Intelligent

Insights

THE EU DIGITAL SERVICES ACT THROUGH A GDPR LENS: THE EDPB'S NEW DRAFT GUIDELINES

Oct 01, 2025

On 11 September 2025, the European Data Protection Board ("**EDBP**") published draft guidelines ("**the Guidelines**") on how to approach both Digital Services Act (**DSA**) compliance obligations and those mandated by the EU General Data Protection Regulation (**GDPR**). The Guidelines raise some interesting points for intermediary service providers (primarily online platforms and hosting service providers) but also provide clarity on compliance with both regulatory frameworks when processing personal data. We set out below the key takeaways from the Guidelines on content moderation, complaint handling, deceptive design patterns, advertising transparency, profiling and protection of minors.

> Cooperation between Digital Services Coordinators, the European Commission and data protection authorities (…) is fundamental to ensure a coherent application of the DSA and the GDPR.

DETECTION AND IDENTIFICATION OF ILLEGAL CONTENT

Whilst the DSA does not impose general monitoring obligations on providers, it anticipates that they may undertake voluntary efforts to detect, identify, and address illegal content. These investigations will often involve the processing of a significant volume of personal data through deployment of various techniques, including use of machine learning ("ML") models and automated content analysis. The EDPB emphasises in this context that both the training and deployment of such ML models to detect and identify illegal content needs to be considered in light of GDPR principles (such as the minimisation principle) and data protection by design and by default obligations. It identifies the fairness and accuracy risks posed by use of these technologies, given current error rates of some pattern recognition tools remain high, and that, for the larger platforms, even a low error rate could lead to a high absolute number of errors (and could expose data subjects to harm, if their accounts are suspended on the basis of wrong or inaccurate results or if their freedom of expression is restricted in error).

For voluntary own-initiative investigations, providers will usually have to rely on Article 6(1)(f) GDPR (legitimate interests) as the legal basis for carrying out the processing, since they are not legally

required to undertake such processing. When conducting the legitimate interests assessment, providers should consider whether the processing would be reasonably expected by data subjects, and whether it concerns children. They should also take all necessary steps to inform data subjects about the reason for the processing, and about the concrete measures which will be used to detect, identify and remove (or disable access to) illegal content in line with the data minimisation principle.

By contrast, when processing is *required* to comply with existing legal obligations (such as copyright take-down requirements), Article 6(1)(c) GDPR may serve as the appropriate legal basis. However, the EDPB stresses that such legal obligations must be clear, precise, and foreseeable, with processing limited to what is strictly necessary and proportionate (i.e. there must be no other less intrusive means which could be used). And to the extent a provider is conducting the processing in response to an order from a competent authority to tackle illegal content or identify a service recipient, it must check any such order meets the requirements of Articles 9 or 10 of the DSA, to enable it to rely on Article 6(1)(c) GDPR.

Providers will also need to balance how to deploy automated processing or profiling techniques, given the Article 22 GPDR prohibition on automated processing where there is no meaningful human involvement or if the human draws strongly on the system's algorithmic recommendation to remove the content. Key will be whether there is any EU or national member state law which would enable a provider to use automated decision-making technologies (although this will not be possible in respect of special category data unless the further GDPR safeguards are met) and that the provider meets the additional transparency requirements and undertakes the required DPIA.

NOTICE AND ACTION MECHANISMS

The implementation of the notice and action mechanisms required under the DSA is likely to imply the processing of personal data of a notifying individual as well as the affected recipient of the service. The EDPB therefore reminds providers that personal data processed should be limited to those necessary for the specific DSA purposes and that the notification process should allow but not require the identification of the notifier unless necessary to determine if the content is illegal. Again, automated management of notices will require a provider to meet Article 22 GDPR safeguards and ensure users are aware of the use of automated decision-making tools for this purpose.

COMPLAINT-HANDLING

The EDPB notes that the DSA allows for account suspension of users who frequently provide manifestly illegal content or frequently submit manifestly unfounded complaints and that this step is to be taken under the supervision of appropriately qualified staff (and not solely on the basis of automated means). In this context, providers will need to be mindful of the GDPR accuracy

principle, to avoid suspensions based on processing of inaccurate personal data and only strictly necessary data is processed.

DECEPTIVE DESIGN PRACTICES

The EDPB identifies the separate zones of competence for the DSA and the GDPR in relation to deceptive design patterns used by online platforms, with the GDPR in play when personal data is being processed and when the data subject's behaviour that the pattern is influencing relates to the processing of personal data.

TRANSPARENCY WHEN ADVERTISING

The EDPB guidelines distinguish between DSA and GDPR transparency timelines: while GDPR requires information provision at the time personal data is collected (or before, if processing for advertising purposes is based on consent), DSA transparency information has to be presented in real-time when advertisements are served to the service user. Additionally, Article 26 DSA information must be directly accessible from an advertisement, whereas GDPR transparency information may be provided through a privacy policy.

The processing involved in the presentation of adverts to particular users may involve elements of automated decision-making, if it produces legal effects or similarly significantly affects data subjects. Factors to consider include the intrusiveness of profiling, cross-platform tracking, user expectations, delivery methods, and exploitation of user vulnerabilities.

The prohibition on using special categories of data for profiling-based advertising under Article 26(3) DSA complements but goes beyond GDPR restrictions. The DSA prohibition applies even where providers could rely on an appropriate legal basis under Articles 6(1) and 9(2) GDPR.

PROFILING

The EDPB recognises the utility of the recommender systems used by those platforms who have a large catalogue of content, but notes the risk where platforms might make use of automated personal data processing to personalise recommendations, for example, the processing of personal data on a large scale, potential lack of accuracy and transparency concerning inferences and combination of personal data, evaluation or scoring (profiling), and the processing of special categories of data or data of highly personal nature or data of vulnerable data subjects. As a result, GDPR principles apply (including the principles of lawfulness, fairness and transparency, purpose limitation, and accuracy) and there is a requirement to identify an appropriate legal basis under Article 6(1) GDPR to profile data subjects. Platforms will also need to consider if the use of a recommender system effectively operates as an automated processing, if the algorithmic processes could propose content, services and products that significantly affect individuals having a prolonged or permanent impact on them or significantly affect their behaviour or choices.

Providers must therefore clarify in their terms of service, using an easy understandable form, why certain information is suggested or prioritised, setting out the main parameters influencing the suggestions. Where the provider of the online platform provides several options for recommender systems to users, the provider must also let users have some amount of control on recommendations they receive.

PROTECTION OF MINORS

> The safety and security of minors in online platforms is a major and growing concern that must be balanced with the need to respect the privacy and the protection of personal data of all users of online platforms.

The DSA obliges platforms to take appropriate measures to protect minors and also assess how they should process the personal data of minors (for example, if required in the context of age assurance measures). The EDPB considers that the assurance of the age of a person can also take place without identification of the respective user by the platform. Therefore, providers of online platforms should in particular avoid age assurance mechanisms that enable unambiguous online identification of their users. If a provider decides to implement age assurance measures, following an assessment, it must take a risk-based approach when ensuring that minors cannot access the platform and prevent potentially adverse effects for all recipients of the service, including by limiting the processing of users' personal data to what is necessary and proportionate to estimate or verify their age (e.g., if an age range provides reasonable certainty that the recipient of the service is a minor, the exact date of birth should not be verified). Platforms should not estimate or verify and permanently store the age or age range of the service user, but just record whether the recipient of the service fulfils the conditions to use the service (following the principles of data minimisation and data protection by design and by default).

RELATED CAPABILITIES

- AdTech
- Data Privacy & Security
- General Data Protection Regulation
- Regulation, Compliance & Advisory

MEET THE TEAM

Geraldine Scali

Partner and EMEA Lead of Data Privacy and Security, London

geraldine.scali@bclplaw.com
+44 (0) 20 3400 4483

Anna Blest

Knowledge & Innovation Counsel, London

anna.blest@bclplaw.com
+44 (0) 20 3400 4475
