CUATRECASAS

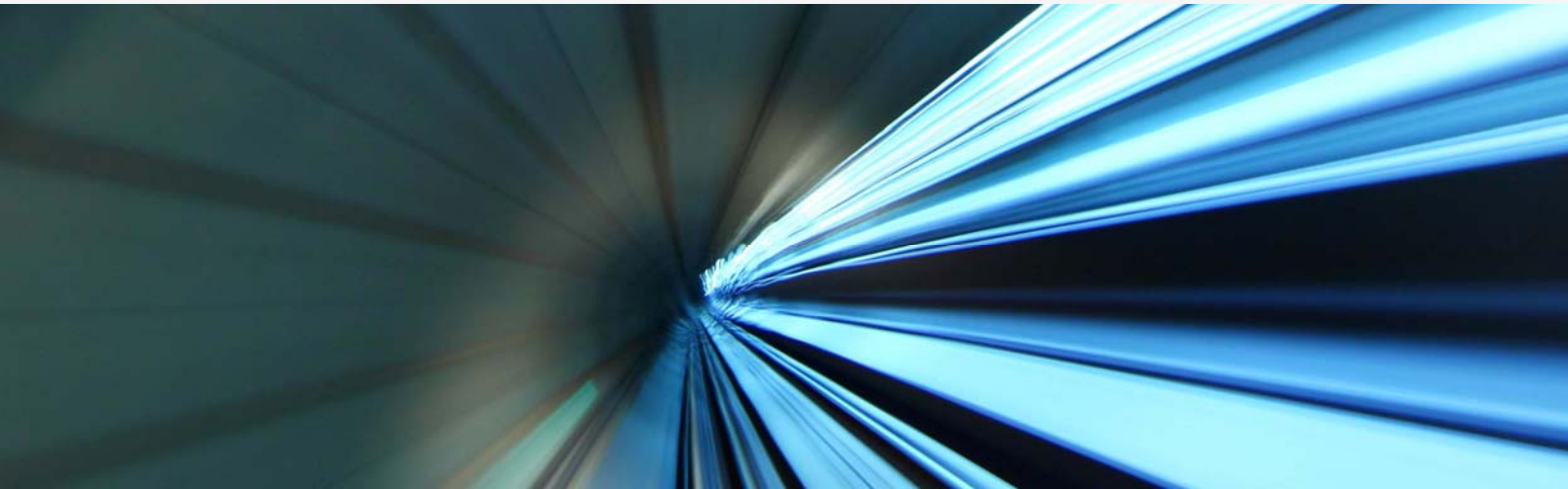
EDPB adopts guidelines on the interplay between the DSA and the GDPR

The European Data Protection Board adopts first guidelines on the interplay between the Digital Services Act and the General Data Protection Regulation

European Union | Legal Flash | October 2025

KEY ASPECTS

- Simultaneous compliance with the DSA and the GDPR is essential for intermediary service providers, requiring that the processing of personal data observes the principles of lawfulness, minimization and transparency.
- The obligation to carry out a Data Protection Impact Assessment (DPIA) applies in high-risk situations, such as voluntary investigations or in the management of complaints.
- Transparency in recommendation systems implies the provision of options not based on profiling and the limitation of the time it takes to retain users' choices to what is strictly necessary.
- Systemic risk management and mitigation, especially for *Very Large Online Platforms* (*VLOPs*) and *Very Large Online Search Engines* (*VLOSEs*), require the implementation of measures that are proportionate and compatible with the requirements of the GDPR.



EDPB's First Step on the Relationship Between DSA and GDPR

On 12 September 2025, the European Data Protection Board (EDPB) published the first draft guidelines on the interplay between Regulation (EU) 2022/2065 of 19 October 2022 (Digital Services Act, hereinafter referred to as "DSA") and Regulation (EU) 2016/679 of 27 April 2016 (General Data Protection Regulation, hereinafter referred to as the "GDPR"), entitled "Guidelines 3/2025 on the interplay between the DSA and the GDPR".

The publication of the Guidelines 3/2025 is a crucial step in clarifying how online service providers should apply the GDPR in the context of their obligations under the DSA. This regulatory framework follows discussions on the topic, which were initiated and deepened in previous plenary sessions of the EDPB, including its 99th session, held between 2 and 3 December 2024[1].

In those sessions, the EDPB underlined the need for greater alignment and cooperation between regulatory authorities to ensure a consistent and harmonized application of the GDPR and the new European Union (EU) digital legislation[2], including the DSA. In this sense, it is important to recall that the application of the DSA is without prejudice to Union law on the protection of personal data, in particular, the GDPR and Directive 2002/58/EC (Directive on privacy and electronic communications), as provided for in Article 2(4)(g) of the DSA.

In this publication, after presenting the legal framework that relates the DSA and the GDPR, we focus on some of the key points of the EDPB draft guidelines that harmonize the application of both regulations, highlighting the implications and good practices that organizations can follow to ensure compliance with both the DSA and the GDPR.

Note: The Guidelines are under review and under public consultation until October 31, 2025.

Legal framework: the DSA and the GDPR

DSA

The **DSA** aims to establish harmonised rules for a safe, predictable and reliable online environment in the internal market, effectively protecting the fundamental rights of internet users. It applies to intermediary service providers, which include "mere conduit", "caching" and "hosting" services. The DSA has a broad territorial scope and applies to providers offering services in the Union, regardless of their place of establishment, provided that there is a substantial link to the Union.

GDPR

In turn, the **GDPR** establishes the rules for the protection of natural persons with regard to the processing of their personal data, a fundamental right enshrined in the Charter of Fundamental Rights of the EU. It considers applies to the processing of data of data subjects who are in the Union, even if the controller or processor is not established in the EU. The GDPR is based on principles such as lawfulness, fairness, transparency, minimization and accuracy, and accountability regarding the processing of personal data.

[1] https://www.edpb.europa.eu/system/files/2024-11/20241202-03plenagenda_public.pdf.
[2] https://www.edpb.europa.eu/system/files/2024-12/edpb_statement_20241203_ec_2nd_gdpr_evaluation_report_en.pdf.

The EDPB Guidelines: Interplay between the DSA and the GDPR

As mentioned above, the EDPB Guidelines are crucial in navigating the complexity resulting from the simultaneous application of both regulations. The DSA makes several explicit references to GDPR concepts, such as "profiling" (Article 4(4) GDPR) and "special categories of personal data" (Article 9(1) GDPR). The EDPB Guidelines address the interpretation and application of the GDPR in these and other contexts.

Some of the most relevant points of interplay stand out, as detailed in the EDPB guidelines:

Voluntary Own-Initiative Investigations and Legal Compliance (Article 7 of the DSA)

- In Articles 4 to 8, the DSA establishes exemptions from liability for digital service providers, under certain conditions, provided that they do not have actual knowledge of illegal content or are not aware of obvious circumstances of illegality.

- Article 7 of the DSA allows intermediary service providers to carry out voluntary investigations to detect and combat access to illegal content, without losing their disclaimers, provided that they act in good faith and diligently.

- However, the EDPB guidelines reinforce that this provision does not impose a general monitoring or active fact-finding obligation on providers of intermediary services, which is indeed prohibited by Article 8 of the DSA.

- The EDPB explains that, as far as possible, these investigations should not involve the processing of any personal data. In any case, if it is necessary to carry out such processing, it is important to ensure compliance with the GDPR, including the principles of lawfulness (Article 6 of the GDPR) and data minimisation (Article 5(1)(c) of the GDPR).

- Indeed, as foreseen in the Guidelines, digital service providers may cover the processing of data by:
    - The existence of a legitimate interest (Article 6(1)(f) of the GDPR), provided that the necessity of the processing is justified against the fundamental rights of individuals, and the provider is transparent about the measures adopted;
    - Unless the review is carried out to comply with the requirements of Union law and national law in compliance with Union law, in which case the legal basis will be compliance with a legal obligation (Article 6(1)(c) of the GDPR).

- Providers must also clearly inform users about such investigations, not only in accordance with the terms of Articles 12 to 14 of the GDPR (through the typical privacy policy), but also through transparency reports and terms and conditions, provided for in Articles 14(1) and 15(1)(c) of the DSA. Since the conduct of such investigations is not, under the DSA, an obligation, the EDPB indicates as the most appropriate lawful basis the legitimate interests of the service provider concerned, unless it entails compliance with a legal obligation not imposed by the DSA, such as companies that are required to identify and remove copyright-protected works on online content-sharing services, in accordance with Directive 2019/790 on Copyright in the Digital Single Market.

- Another relevant point in the eyes of the EDPB (*see* Point 24. of the Guidelines) is whether the online service providers have automatic systems in place for the analysis and removal of illegal content. As the EDPB recalls, users (as data subjects in light of the GDPR) have the right not to be subject to a decision based solely on automated processing, which produces legal effects on it or similarly significantly affects them. In such cases, the EDPB understands that it is

essential to carry out a Data Protection Impact Assessment (DPIA)of the system in order to assess the degree of automation and whether the same automation can significantly affect the rights of users.

- Best practices: A hosting service platform may implement systems to proactively detect and combat the presence of illegal content. Although it is a voluntary action to combat illegality, any collection and analysis of personal data involved must comply with the principles of the GDPR. The platform must ensure that the processing is lawful, and that the data is minimized to what is strictly necessary. In addition, given the potential high risk, it should carry out a DPIA and, if necessary, consult the supervisory authority.

Notice-and-Action Mechanisms (Articles 16 and 17 of the DSA)

- Hosting service providers should put in place notice-and-action mechanisms that allow any person or entity to flag allegedly illegal content. These mechanisms should be easily accessible and simple to use. Sufficiently precise and adequately substantiated notifications give rise to "actual knowledge" of illegality (for the purposes of Article 6 of the DSA). In parallel, they shall prepare a clear and specific statement of reasons to all affected service recipients in relation to restrictions imposed.

- If these processes involve the processing of personal data, the provider of intermediary services will be qualified as a controller.

- Best practices: Any processing of personal data associated with these mechanisms should be carried out in accordance with the GDPR, ensuring minimisation of the data collected (Article 5(1)(c) of the GDPR) and proportionality in the actions taken, as underlined in Point 30. of the guidelines. This includes ensuring that only data that is strictly necessary is processed to assess the legality of the content.

Processing of Personal Data of the Affected Recipients by Providers of Online Platforms for Handling of Complaint and Combatting Misuse (Articles 20 and 23 of the DSA)

- Online platform providers act as controllers in relation to personal data processed in these contexts.

- The DSA requires that claims management decisions be made under the supervision of suitably qualified employees, and not solely on the basis of automated means.

- The EDPB guidelines recall that the complaint mechanism of Article 20 of the DSA is without prejudice to the rights and remedies available to data subjects under the GDPR.

- Best practices: When establishing their anti-abuse policies, online platform providers should ensure that they comply with all the data protection principles of Article 5 of the GDPR, including data minimisation, accuracy, transparency and retention, as set out in Section 41 of the guidelines. The DSA provides safeguards against abuse, such as the temporary suspension of services after prior notice and case-by-case analysis, assessed on a case-by-case basis and in a timely, diligent and objective manner.

Dark patterns (Article 25 DSA)

- Article 25 of the DSA) is designed to protect users from deceptive tactics on digital platform interfaces, called deceptive design patterns. These practices manipulate users into making harmful decisions, such as sharing more data than necessary or investing too much time on the platform, as well as *infinite scrolling, autoplay, and timers, which can lead to addictive behaviors.*

- The DSA is designed to require online platform services to enable users to make informed and autonomous decisions. However, as the EDPB recalls, the prohibition in Article 25 does not apply to practices covered by the GDPR or Directive 2005/29/EC.

- In this regard, in the event that dark patterns involve the processing of personal data (e.g. patterns that manipulate the user to provide additional personal information), the competent authority will be the data protection authority.

Transparency in advertising and prohibition of the presentation of advertisements based on profiling using special categories of data (Article 26 of the DSA)

- Broadly speaking, Article 26 of the DSA sets out transparency rules for online platform providers in relation to advertising and prohibits such providers from presenting ads to recipients based on profiling using special categories of data, as mentioned in Article 9(1) of the GDPR.

- It should be recalled that Recital 68 of the DSA clarifies that the requirements set out in Article 26 of the DSA do not affect compliance with the GDPR and that the provisions of the ePrivacy Directive remain applicable (which, in Spain, has been transposed by both the LSSI and the LGTel).

- In any case, the EDPB recalls that online service providers must comply with both the reporting obligation set out in Article 26 of the DSA and the reporting and transparency obligations of Articles 13 and 14 of the GDPR; that is, both when the data is provided directly by users and not.

- In line with what has been analysed above for Article 7 of the DSA, the EDPB also makes reference to automated decision-making and the right of users under Article 22 of the GDPR. This comment also extends to possible automated decisions taken within recommendation systems (Article 27 of the DSA).

- Therefore, both the DSA and the GDPR include transparency obligations relevant to ad serving and recommendation systems on online platforms.

Recommender Systems (Articles 27 and 38 of the DSA)

- Providers of online platforms using recommender systems should be transparent about the main parameters used and offer options that allow service recipients to influence those parameters, as required by Article 27 of the DSA.

- *VLOPs* and *VLOSEs* must offer at least one option for each of their recommender systems that is not based on profiling as defined in Article 4(4) of the GDPR. This obligation is provided for in Article 38 of the DSA. These choices should be directly accessible from the *online* interface where the recommendations are presented.

- The EDPB guidelines reiterate the importance of integrating the principle of "data protection by design and by default" (Article 25 of the GDPR) when designing recommender systems, referring to the "EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default".

- In Point 88. of the guidelines, the EDPB underlines that the collection and processing of users' choices regarding the modification of the parameters of recommender systems should be processed by platform providers and online search engines only for the purpose of complying

with the DSA and stored only for as long as necessary, without retaining history of previous choices.

- Best practices: Platform developers and operators should design their recommender systems with privacy in mind, ensuring transparency and options that respect user autonomy, including non-profile-based options for *VLOPs* and *VLOSEs*.

Risk Assessment and Mitigation (Articles 34 and 35 of the DSA)

- Articles 34 and 35 of the DSA require *VLOPs* and *VLOSEs* to manage systemic risks, which have negative effects on fundamental rights (including Articles 7 and 8 of the Charter, i.e. the right to respect for private life and the protection of personal data), public health and minors.

- The EDPB guidelines, in paragraph 101, highlight that the DPIA, under Article 35 of the GDPR, is a crucial tool to identify and mitigate risks to the rights and freedoms of data subjects, especially for *VLOPs* and *VLOSEs*.

- The measures to inform users, referred to in Article 35(1)(i) of the DSA, are consistent with the obligations of Articles 13 and 14 of the GDPR, such as the obligations of information and transparency, to the extent that personal data is processed.

- Best practices: The illustrative measures provided for in Article 35 of the DSA, which aim to mitigate systemic risks such as the dissemination of illegal content or the impact on fundamental rights and democratic processes, are extremely useful for providers and supervisory authorities, as highlighted in Points 100. and 106. of the EDPB guidelines. These should be considered in the DPIA under Article 35 of the GDPR, underlining that all risk assessment and mitigation measures should be reasonable, proportionate and effective, and fully compatible with the GDPR's principles of lawfulness and data minimisation. The proactive approach includes the analysis of algorithmic systems, content moderation and advertising practices to prevent or minimize bias and ensure respect for users' rights.

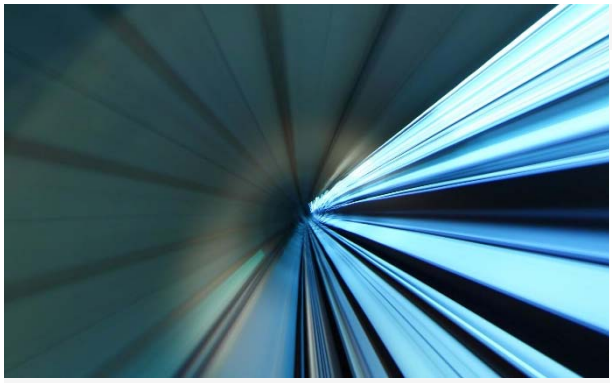
The Importance of the EDPB Guidelines

The adoption of the EDPB Guidelines on the interplay between the DSA and the GDPR represents an important step towards ensuring **legal certainty** and the **protection of fundamental rights** for any company operating in the European digital ecosystem.

These Guidelines provide the **necessary clarity** for intermediary service providers, in particular online platforms and online search engines, to strengthen their internal mechanisms and compliance strategies.

By aligning their operations with the requirements of both regulations, these entities will contribute to a more **transparent, accountable and privacy-friendly digital ecosystem** for their users, boosting **trust** and **innovation** in the Digital Single Market.

The consultation is open until October 31, 2025.



For additional information on the content of this document, you can send an email to our Knowledge and Innovation team or contact your usual contact at Cuatrecasas.