EU Digital Laws: Mapping the Interplays with the GDPR

Digital Services Act: General Data Protection Regulation

The Digital Services Act applies tiered obligations to various classes of intermediary service providers, imposing the strictest rules upon entities designated by the European Commission as very large online platforms and very large online search engines. The DSA aims to create a safe, predictable and trusted online environment by preventing the dissemination of illegal content, reducing societal risks stemming from the spread of disinformation and preserving fundamental rights. These aims are complementary to those of the EU General Data Protection Regulation, which seeks to protect the fundamental rights of data subjects. To better harmonize the overlapping obligations of the DSA and GDPR, the European Data Protection Board has adopted formal guidelines on their interplay.

DSA		GDPR
Article 7 ISPs may carry out voluntary investigations of their own initiative and take measures to detect, identify remove and/or disable access to illegal content online.	Detecting, identifying and addressing illegal content	**Articles 5 and 6(1)(c, f)** Processing of personal data under Article 7 DSA must observe the principles of Article 5 GDPR and other obligations of controllers. Legitimate interests may serve as the most appropriate legal basis for ISPs to process personal data to develop measures to detect, identify and disable illegal content.
Articles 16-17 and 22 Providers of hosting services, including online platforms, have an obligation to put in place "notice and action" mechanisms that allow individuals or entities to electronically notify them of the presence of specific information items they consider to be illegal content. These can also be triggered by "trusted flaggers."	Notice and action mechanisms	**Articles 5(1)(c) and 13** Personal data collected from the notifier should be limited to what is necessary for this specific purpose and generally not beyond what is referred to in Article 16(2) DSA. If the notifier's personal data is communicated to the affected recipient of the service, the notifier (i.e., the data subject) should be kept informed.
Articles 20 and 23 Providers of online platforms may be required to carry out further processing of personal data in order to comply with their obligations to provide recipients of their service, as well as individuals and entities that have submitted a notice via Article 16 DSA, with an internal complaint-handling system, and suspend the provision of their services to recipients that frequently provide illegal content.	Complaint-handling systems and account suspensions	**Articles 5 and 12-14** When providers of online platforms act as controllers in conducting their Article 20 DSA obligations, they should respect the rights and remedies available to data subjects pursuant to the GDPR, in particular the principles of data minimization, accuracy, transparency and data retention.
Article 25 and Recitals 67, 81 and 83 Article 25(1) DSA requires providers of online platforms to avoid the use of deceptive design patterns in their interfaces, but, according to Article 25(2) DSA, this prohibition does not apply to the practices of providers covered by the GDPR or by the Unfair Commercial Practices Directive.	Deceptive design patterns	**Articles 4(11), 5(1)(a-c), 7, 12 and 25** When assessing whether a deceptive design pattern is covered within the scope of the GDPR, key considerations include whether personal data is being processed and whether the pattern influences a data subject's behavior in relation to that processing of personal data.
Article 26(1) and Recitals 68 and 107 Providers of online platforms must be transparent toward recipients of their services regarding advertisements presented on their interfaces. This information may be provided after the processing of personal data may have occurred.	Transparency	**Articles 13-14** In contrast to Article 26 DSA, Article 13 GDPR requires that information be provided at the time when personal data is obtained before the processing takes place.
Article 26(3) The use of special categories of data to present advertisements based on profiling is prohibited.	Special categories of data, profiling	**Articles 4(4), 6(1), 9(1-2) and 22(4)** The prohibition on the use of special categories of data applies even in situations where the provider of the online platform would otherwise rely on an appropriate legal basis under GDPR Article 6(1) and an appropriate derogation under GDPR Article 9(2) for its processing.
Articles 3(s), 27 and 38 When providing different options for recommender systems to users, providers of online platforms should not nudge users to select the option for a recommender system that is based on profiling.	Recommender systems	**Articles 4(4) and 22(1)** VLOPs and VLOSEs that use recommender systems must provide at least one option not based on profiling as defined under GDPR Article 4(4). The presentation of specific content to a user of an online platform via a recommender system would be considered a "decision" within the meaning of GDPR Article 22(1), especially when it can have serious consequences for individuals.
Article 28(1-2) When putting in place measures to ensure a high level of privacy, safety and security for minors (e.g., age assurance), providers of online platforms may rely on Article 28(1-2) of the DSA as a legal basis for the processing of personal data under GDPR Article 6(1)(c).	Privacy, safety and security of minors	**Articles 4(4), 6(1)(c) and 6(3)** Processing personal data under Article 28 DSA must still adhere to the general requirements of the GDPR and the controller must demonstrate that such processing is necessary and proportionate.
Articles 34-35 VLOPs and VLOSEs must manage systemic risks of their services, including risks to fundamental rights such as privacy and the protection of personal data.	Managing systemic risks	**Articles 5(1)(c), 25 and 35** Data minimization and data protection by design and by default may contribute to the management of systemic risks by VLOPs and VLOSEs. Under Article 35 GDPR, a data protection impact assessment is likely to be required if a systemic risk is identified.
Articles 49(1-2) and 64(3) and Recitals 109 and 143 Cooperation may occur between Digital Service Coordinators and data protection supervisory authorities to ensure consistent application of the DSA and GDPR. The Commission may appoint experts or auditors from the data protection authorities to assist in monitoring implementation of and compliance with obligations of the DSA.	Cooperation amongst authorities	**Article 60** Authorities are recommended to consult one another when called upon to examine whether the conduct of an intermediary service provider, controller or processor is consistent with the legal framework under the other authority's supervision. When a competent authority enforcing the DSA consults a data protection supervisory authority, the latter should inform the DSA-enforcing authority if it intends to initiate the cooperation procedure vis-à-vis GDPR Article 60 to determine the consistency of the conduct in question with the GDPR.

Published March 2026.

iapp.org