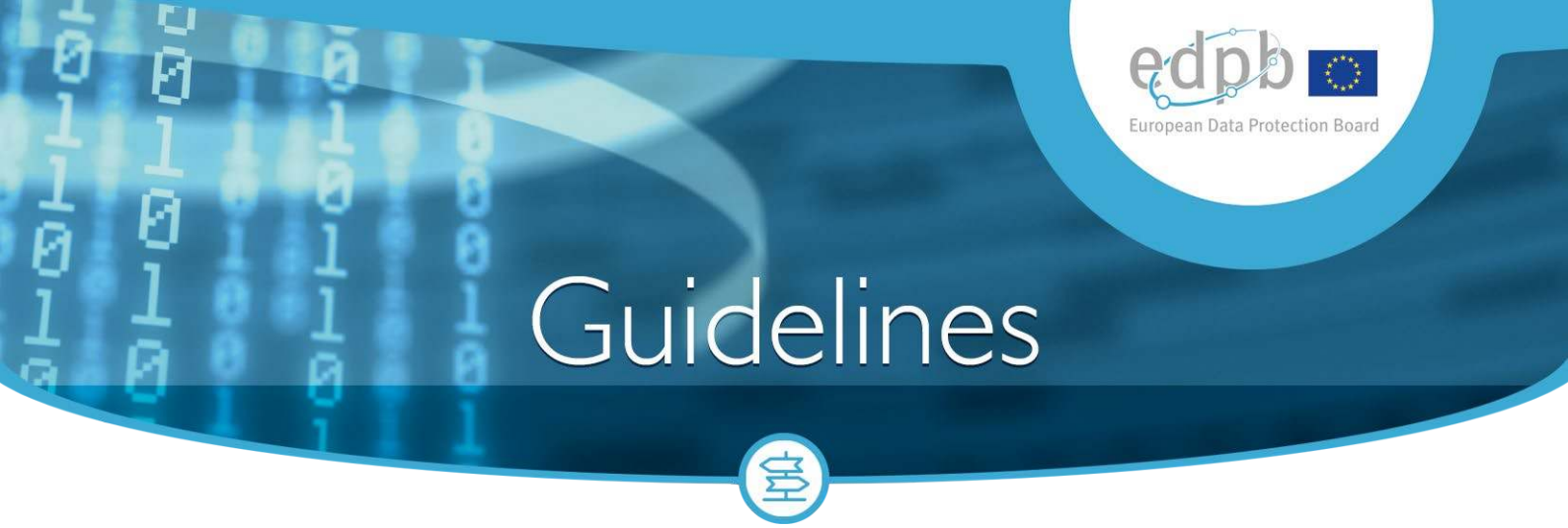

Guidelines 3/2025

on the interplay between the DSA and the GDPR

Version 1.0

Adopted on 11 September 2025

Executive summary

The Digital Services Act (DSA) sets out various rules and obligations for intermediary service providers. While the DSA is subject to interpretation by the competent authorities under the DSA, the European Board for Digital Services (EBDS), and EU courts, there are a number of provisions that relate to the data protection legal framework, such as rules that refer to 'profiling' and 'special categories of data' in the meaning of the GDPR, and have implications for the processing of personal data by intermediary service providers.

Coherent interpretation and application of the DSA and the GDPR by the competent supervisory authorities under each regulation, as well as adequate mechanisms to ensure this consistency, are important to provide legal certainty for intermediary service providers and ultimately to protect the rights and freedoms of data subjects.

These guidelines aim to contribute to the consistent interpretation and application of the DSA and of the GDPR insofar as some provisions of the DSA concern the processing of personal data by intermediary service providers and include references to GDPR concepts and definitions. The guidelines focus on specific provisions of the DSA where there is a significant interplay with the GDPR.

The guidelines recognise that efforts to detect, identify, and address (e.g., de-monetise, remove or disable access to) illegal content under Article 7 DSA may involve processing of personal data using different techniques. In addition to highlighting specific risks for individuals that should be mitigated in the context of content moderation, the guidelines clarify under which conditions Article 6(1)(c) or (f) GDPR may serve as a lawful basis for measures to detect, identify and disable illegal content, including by offering examples.

Notice and action mechanisms and internal complaint-handling systems required by the DSA may also require the processing of personal data, notably since service providers must implement mechanisms for reporting illegal content. Hosting providers should only collect necessary personal data and the notification mechanism should allow, but not require, the identification of the notifier, unless identification is necessary for determining whether information constitutes illegal content. If it is necessary to reveal the notifier's identity to the affected recipients of the service, the notifier should be duly informed. The complaint mechanism under Article 20 DSA and the suspension of an account under Article 23 DSA are without prejudice to the rights and remedies available to data subjects pursuant to the GDPR vis-à-vis providers of online platforms acting as controllers.

Article 25(2) DSA provides that the prohibition of Article 25(1) DSA for providers of online platforms to deploy deceptive design patterns in their interfaces shall not apply to practices of those providers that are covered by the GDPR. The guidelines mention key elements to consider when assessing whether a deceptive design pattern is covered by the GDPR, in particular whether personal data is being processed and whether the data subject's behaviour that the pattern is influencing relates to the processing of personal data. Such key elements are complemented by examples of cases where deceptive design patterns are or are not covered by the GDPR.

Article 26 DSA mandates providers of online platforms to be transparent towards recipients of their services regarding advertisements they present on their interfaces, and prohibits the use of special categories of data to present advertisements based on profiling. Whereas information provided under Article 26 DSA would be provided after processing of personal data may have occurred, transparency under Article 13 GDPR requires information to be provided at the time when personal data is obtained. The prohibition on the use of special categories of data under Article 26(3) DSA complements the prohibitions under Articles 9(1) and 22(4) GDPR, and applies even in situations where the provider

of the online platform would rely on an appropriate legal basis under Article 6(1) GDPR and an appropriate derogation under Article 9(2) GDPR for its processing.

Providers of online platforms may use personal data of their users in their recommender systems to personalise the order or prominence of the content shown to them. Recommender systems raise concerns about the accuracy and transparency of inferences and combination of personal data, and potential risks associated with large-scale and/or sensitive personal data processing. The EDPB notes that it cannot be excluded that the presentation of specific content to users of an online platform via a recommender system would be a 'decision' in the meaning of Article 22(1) GDPR, notably when they can have serious consequences for individuals. When providing different options for recommender systems to users, providers of online platforms should present options equally and should not nudge users to select the option for a recommender system that is based on profiling. While the non-profiling based option is active, the provider of the online platform should not continue to collect and process personal data to profile the user.

The EDPB welcomes the objective of the DSA of ensuring a high level of privacy, safety and security for minors using online platforms. The guidelines acknowledge that Articles 28(1) and (2) DSA can qualify as a legal basis for processing personal data under Article 6(1)(c) GDPR, provided such processing is necessary and proportionate, which is for the controller to demonstrate. 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. Therefore, the EDPB considers that providers of online platforms should in particular avoid age assurance mechanisms that enable unambiguous online identification of their users, and should not estimate or verify and permanently store the age or age range of the recipient of the service as a result of their age estimation process.

Articles 34 and 35 DSA require providers of very large online platorms and online search engines to manage systemic risks of their services, including the dissemination of illegal content and risks to on fundamental rights such as privacy and the protection of personal data. Appropriate implementation of data minimisation and data protection by design and by default requirements under the GDPR may contribute to address systemic risks identified in these services. If systemic risks are identified, a data protecton impact assessment is likely to be mandatory under the GDPR.

The EDPB believes it is important to clarify the relationship between codes of conduct developed under the DSA and the GDPR, and to ensure involvement of data protection authorities when developing the latter, where appropriate.

Cooperation between Digital Services Coordinators, the European Commission and data protection authorities - even if the latter are not designated as competent authorities under the DSA at Member State level - is fundamental to ensure a coherent application of the DSA and the GDPR. The principle of sincere cooperation requires such authorities to cooperate, meaning that they should consult each other when they are called upon to examine whether the conduct of an intermediary service provider, a controller or a processor is consistent with the provisions of the framework under the other's supervision. Mutual consultation is important to enhance legal certainty and avoid regulatory incon-sistencies and risks related to ne bis in idem in the application of both frameworks.

Table of contents

The European Data Protection Board

Having regard to Article 70 (1)(e) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, (hereinafter "GDPR"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018[1],

Having regard to Article 12 and Article 22 of its Rules of Procedure,

HAS ADOPTED THE FOLLOWING GUIDELINES ON THE INTERPLAY BETWEEN THE DSA AND THE GDPR

1 INTRODUCTION AND SCOPE OF THE GUIDELINES

1. Regulation (EU) 2022/2065[2] (the 'Digital Services Act' or 'DSA') fully harmonises the rules applicable to intermediary services in the internal market with the objective of ensuring a safe, predictable and trusted online environment, addressing the dissemination of illegal content online and the societal risks that the dissemination of disinformation or other content may generate, and within which fundamental rights enshrined in the EU Charter of Fundamental Rights ('the Charter') are effectively protected.[3] The DSA was adopted on 19 October 2022 and became fully applicable on 17 February 2024, although some of the DSA's provisions started applying already on 16 November 2022.[4] Among the various intermediary services providers in scope of the DSA, providers of Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs) have four months from the date of their designation by the European Commission as such to comply with specific obligations. The current VLOPs and VLOSEs designated by the European Commission can be found on the European Commission website.[5]

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).[6] As a result, both the DSA and the GDPR may cover

[1] References to "Member States" made throughout this document should be understood as references to "EEA Member States".
[2] Regulation (EU) 2022/2065 of the European Parliament and the Council on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act), OJ L 277, 27.10.2022, p. 1.
[3] Recital 9 DSA.
[4] Article 93 DSA.
[5] European Commission, Supervision of the designated very large online platforms and search engines under DSA, https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses.
[6] See Articles 4(7) and (8) GDPR, as well as EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.1, Adopted on 7 July 2021.

processing activities of the same entities. The DSA imposes obligations on the various types of intermediary services providers covered by the DSA (notably, mere conduit, caching and hosting service providers) that require varying levels of personal data processing activities. In this regard, the DSA imposes a significantly higher number of obligations on a subcategory of hosting service providers, notably providers of online platforms.[7] Moreover, both online platforms and online search engines, when having a number of average monthly active recipients of the service in the EU equal to or higher than 45 million, can be designated by the European Commission as VLOPs or VLOSEs respectively.[8] From that status, they are required to comply with additional obligations that are listed under Section 5 of Chapter III of the DSA[9] and that require additional processing of personal data.

3. A number of provisions of the DSA specifically refer to the protection of personal data as well as definitions and concepts under the GDPR, such as 'profiling' and 'special categories of data', though in the context and for the purpose of the implementation of the specific DSA regulatory objectives under the oversight of competent authorities under the DSA.

4. Ensuring the coherent interpretation and application of the DSA and the GDPR by providers that are covered by both Regulations is important. This is particularly the case where provisions of the DSA affect the processing of personal data by intermediary service providers and specifically refer to definitions and concepts under the GDPR. For example, Articles 28(2) and 26(3) DSA refer to the definition of profiling under Article 4(4) GDPR when imposing prohibitions concerning certain types of advertisements by online platforms. The prohibition contained in Article 26(3) also relies on the catalogue of special categories of personal data under Article 9(1) GDPR. Provisions like this - as well as other provisions whose implementation requires processing of personal data by intermediary service providers - should be read consistently with the provisions of the GDPR and the ePrivacy Directive, when applicable.[10]

5. The objective of the present guidelines is to clarify how intermediary service providers should interpret and apply the GDPR when processing personal data in the contexts covered by the DSA. The goal of the guidelines is not to interpret the DSA as such, which is for competent authorities under the DSA

[7] According to Article 3(i) DSA, an 'online platform' "*means a hosting service that, at the request of a recipient of the service, stores and disseminates information to the public, unless that activity is a minor and purely ancillary feature of another service or a minor functionality of the principal service and, for objective and technical reasons, cannot be used without that other service, and the integration of the feature or functionality into the other service is not a means to circumvent the applicability of*" the DSA. Recital 14 clarifies that "*Interpersonal communication services, as defined in Directive (EU) 2018/1972 of the European Parliament and of the Council, such as emails or private messaging services, fall outside the scope of the definition of online platforms as they are used for interpersonal communication between a finite number of persons determined by the sender of the communication. However, the obligations set out in this Regulation for providers of online platforms may apply to services that allow the making available of information to a potentially unlimited number of recipients, not determined by the sender of the communication, such as through public groups or open channels. Information should be considered disseminated to the public within the meaning of this Regulation only where that dissemination occurs upon the direct request by the recipient of the service that provided the information*."

[8] Article 33(1) and (4) DSA.

[9] Section 5 of Chapter III DSA sets out additional obligations for providers of very large online platforms and of very large online search engines to manage systemic risks.

[10] Article 2(4)(g) DSA.

(including the European Commission in relation to VLOPs and VLOSEs[11]) - with the support of the European Board for Digital Services ('EBDS')[12] - and EU courts to do. These guidelines aim to contribute to the consistent interpretation and application of the DSA and of the GDPR insofar as some provisions of the DSA concern the processing of personal data by intermediary service providers and include references to GDPR concepts and definitions.

6. Additional data protection-related obligations for political advertising arise from Regulation (EU) 2024/900 on the transparency and targeting of political advertising. Furthermore, the Commission has published a delegated regulation under Article 40(13) DSA laying down the technical conditions under which providers of very large online platforms or of very large online search engines are to share data (including personal data) with researchers under Article 40 DSA.[13] The preceding matters are not part of the present guidelines, and the EDPB will work separately to ensure a consistent application of the GDPR in those contexts.

1.1 The relationship between the DSA and the GDPR

7. The EDPB takes note that the DSA and the GDPR pursue different yet complementary objectives. While the GDPR aims to protect individuals with regard to the processing of personal data, the DSA aims "to contribute to the proper functioning of the internal market for intermediary services by setting out harmonised rules for a safe, predictable and trusted online environment that facilitates innovation and in which fundamental rights enshrined in the Charter, including the principle of consumer protection, are effectively protected"[14].

8. Article 2(4)(g) of the DSA states that the DSA is without prejudice to the rules laid down by other Union legal acts regulating other aspects of the provision of intermediary services in the internal market or specifying and complementing the DSA, in particular the GDPR and the ePrivacy Directive. Recital 10 of the DSA specifies that the protection of individuals with regard to the processing of personal data is governed by the rules of Union law on that subject, in particular the GDPR and the ePrivacy Directive.

9. As a consequence, it is clear that the DSA does not derogate, as *lex specialis*, from the general rules on the processing of personal data under the GDPR nor the rules that particularise the GDPR with respect to the processing of personal data in the electronic communication sector under the ePrivacy Directive.[15] Nonetheless, settled case law of the Court of Justice of the European Union ('CJEU') provides that, where two EU legal acts of the same hierarchical value (such as the DSA and the GDPR) do not

[11] Article 56(2) and (3) DSA.
[12] Article 61(2) DSA states that "*The Board shall advise the Digital Services Coordinators and the Commission in accordance with this Regulation to achieve the following objectives: (a) contributing to the consistent application of this Regulation and effective cooperation of the Digital Services Coordinators and the Commission with regard to matters covered by this Regulation; (b) coordinating and contributing to guidelines and analysis of the Commission and Digital Services Coordinators and other competent authorities on emerging issues across the internal market with regard to matters covered by this Regulation*." See also Article 63(1) DSA.
[13] Commission Delegated Regulation of 1.7.2025 supplementing Regulation (EU) 2022/2065 of the European Parliament and of the Council by laying down the technical conditions and procedures under which providers of very large online platforms and of very large online search engines are to share data with vetted researchers, C(2025) 4340 final.
[14] Article 1(1) DSA.
[15] EDPB Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities, Adopted on 12 March 2019, paragraph 38.

establish priority of one over the other, they should be applied in a compatible manner, which enables a coherent application of them.[16]

10. When monitoring the application of the GDPR by controllers and processors that are also qualified as intermediary service providers under the DSA, data protection supervisory authorities need to take into account the relevant provisions of the DSA (notably, concerning the obligations of the various types of intermediary service providers) with a view to ensuring a compatible and coherent application of EU law in relation to processing activities that are covered by both the GDPR and the DSA. This is particularly the case where the DSA imposes rules that (at least indirectly) concern the processing of personal data by intermediary service providers that are more restrictive than the GDPR itself.

11. In that effort of ensuring coherent application, the EDPB underlines the singular importance that the fundamental right to the protection of personal data has in the context of the Charter and of the TFEU.[17] Therefore, the EDPB deems it important to underline that a consistent and coherent interpretation of the DSA and the GDPR should not lead to lowering the level of protection of the fundamental rights to privacy and data protection as enshrined in primary and secondary EU law. The following sections aim to provide guidance on how to ensure a consistent and coherent application between the GDPR and the main provisions of the DSA that affect the processing of personal data by intermediary service providers.

2 SPECIFIC ISSUES

2.1 Voluntary own-initiative investigations and legal compliance in relation to illegal content (Article 7)

12. Articles 4 to 6 DSA establish liability exemptions for mere conduit, caching and hosting service providers who enable the transmission and/or storage of information, under certain conditions. For example, a hosting service provider that does not have actual knowledge of illegal content and, as regards claims for damages, is not aware of facts or circumstances from which the illegal content is apparent, is not liable for damages suffered by recipients of the service or third parties as a result of the storage (including dissemination, in case the provider is an online platform) of that illegal content.[18]

13. To ensure that liability exemption rules do not remove the incentives for intermediary service providers voluntarily to take measures to detect and tackle illegal content, Article 7 DSA establishes that

---

[16] Judgment of the General Court of 3 May 2018 Malta v Commission, T-653/16, , ECLI:EU:T:2018:241, paragraph 137: "*No provision of Regulations Nos 1049/2001 and 1224/2009 expressly gives one regulation priority over the other. Accordingly, it is appropriate to ensure that each of those regulations is applied in a manner compatible with the other and which enables a coherent application of them (see, by analogy, judgments of 29 June 2010, Commission v Bavarian Lager, C-28/08 P, EU:C:2010:378, paragraph 56, and of 28 June 2012, Commission v Éditions Odile Jacob, C-404/10 P, EU:C:2012:393, paragraph 110).*" Paras 139 and 140 of the judgment also state that, even if "*Article 113(2) and (3) of Regulation No 1224/2009 is not, as such, lex specialis derogating from the general rules on public access to documents laid down in Regulation No 1049/2001*, (...) *the fact remains that, as has been stated in paragraph 137 above, both Regulation No 1049/2001 and Regulation No 1224/2009 should be applied consistently*".

[17] Opinion of Advocate General Szpunar delivered on 11 May 2023 in Case C-33/22 Österreichische Datenschutzbehörde, ECLI:EU:C:2023:397, paragraphs 61 to 78. In particular, paragraph 64 states that "*the right of natural persons to the protection of personal data, enshrined in that provision, is of singular importance compared with the other fundamental rights included in the Charter annexed to the Treaty*".

[18] Article 6(1)(a) DSA.

"*Providers of intermediary services shall not be deemed ineligible for* the *exemptions from liability referred to in Articles 4, 5 and 6 solely because they, in good faith and in a diligent manner, carry out voluntary own-initiative investigations into, or take other measures aimed at detecting, identifying and removing, or disabling access to illegal content, or take the necessary measures to comply with the requirements of Union law and national law in compliance with Union law, including the requirements set out in this Regulation*". However, Article 8 DSA also makes clear that the DSA does not impose - and that EU and Member State law cannot impose - on intermediary service providers general obligations to monitor the information they transmit or store, nor to actively seek facts or circumstances indicating illegal activity.[19]

14. Automated or non-automated own-initiative efforts to detect, identify, and address (e.g., demonetise, remove or disable access to) illegal content or to take the necessary measures to ensure compliance with EU law may involve processing of personal data by intermediary service providers.[20] Such efforts may rely on several different techniques involving processing of personal data, such as the deployment of models based on machine learning (ML) techniques that can recognize the characteristics of a given content item based on the machine's prior learning. These models often require large amounts of data to train on to predict whether a piece of content constitutes illegal content, and can be used for the analysis of shapes, textures, colours and text. In a plaintext setting, multimedia-based or text-based ML tools can be used for detecting illegal content (e.g., through keyword or text pattern matching). Both in the training of such models and in their deployment as part of efforts to detect, identify and address illegal content, providers need to carefully consider, and demonstrate compliance with the principles relating to the processing of personal data (such as the minimisation principle) and data protection by design and by default obligations stemming from the GDPR.[21] Insofar as possible, these actions should not involve any processing of personal data.

15. Technologies for voluntary detection and tackling of illegal content potentially entail the systematic monitoring of data subjects' activities through automated methods that may generate wrong or inaccurate results about a data subject's involvement in abusive practices, which in turn may have significant negative impacts on them (e.g., reputational harm in case of account suspension, restriction of freedom of expression in relation to lawful content, etc.). In data protection terms, the use of these technologies entails fairness and data accuracy risks. These risks are further exacerbated by the fact that the error rates of some existing technologies (such as pattern recognition) tend to be rather high.[22]

---

[19] Similar rules already resulted from Article 15 of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), OJ L 178, 17.7.2000, p. 1–16. See also Judgment of the Court of Justice of 26 April 2022, Poland v Parliament and Council, C-401/19, ECLI:EU:C:2022:297, paragraph 90, and also Judgment of the Court of Justice of 3 October 2019, Eva Glawischnig-Piesczek v Facebook Ireland Limited, C-18/18, ECLI:EU:C:2019:821, paragraphs 41-46.

[20] Such activities are close to - but narrower than - the definition of 'content moderation' under Article 3(t) DSA: "*the activities, whether automated or not, undertaken by providers of intermediary services, that are aimed, in particular, at detecting, identifying and addressing illegal content or information incompatible with their terms and conditions, provided by recipients of the service, including measures taken that affect the availability, visibility, and accessibility of that illegal content or that information, such as demotion, demonetisation, disabling of access to, or removal thereof, or that affect the ability of the recipients of the service to provide that information, such as the termination or suspension of a recipient's account*".

[21] Article 5 and Article 25 GDPR.

[22] European Parliamentary Research Service, Proposal for a regulation laying down the rules to prevent and combat child sexual abuse - Complementary impact assessment, PE 740.248, April 2023, p. 82. See also EDPB-EDPS Joint Opinion 04/2022 on the Proposal for a Regulation of the European Parliament and of the Council laying

Moreover, in some intermediary services - in particular VLOPs and VLOSEs -, given the high number of users and content items shared, even a rather low error rate of technologies for voluntary detection and tackling of illegal content may lead to high absolute numbers of errors.

16. For cases where the processing of personal data will be necessary in order to identify the illegal content, the DSA does not specify to what extent such processing, falling under Article 7 DSA, would be legitimate or proportionate. Therefore, and also in light of the broad definition of 'illegal content' under the DSA,[23] it is important to outline how intermediary service providers may undertake voluntary own-initiative actions under Article 7 DSA in compliance with the GDPR.[24]

17. The first scenario covered by Article 7 DSA is one where intermediary service providers carry out processing in the context of their voluntary own-initiative investigations or other measures to detect, identify and remove (or disable access to) **illegal content**. To comply with the GDPR, this processing must be conducted lawfully, fairly and in a transparent manner towards data subjects,[25] observe the remaining principles of Article 5 GDPR as well as the obligations the GDPR imposes on controllers. First and foremost, intermediary service providers (as controllers) need to identify a legal basis under Article 6(1) GDPR to carry out such processing. Given that controllers are not legally required to carry out processing for these purposes, the most suitable legal basis available in this scenario would be Article 6(1)(f) GDPR ('legitimate interests').

18. To rely on the legitimate interest legal basis, controllers need to fulfil three cumulative conditions:[26] the interest pursued must be legitimate; the processing of personal data must be necessary for the purposes of the legitimate interest pursued; and the interests or fundamental rights and freedoms of the data subjects concerned by the data processing must not override the legitimate interest pursued by the controller. It is clear that the interest of detecting and addressing illegal content in intermediary services to protect the recipients of the service is legitimate, in particular where such content can be disseminated to the public via an online platform.[27] In relation to the other two conditions, controllers

---

down rules to prevent and combat child sexual abuse, Adopted on 28 July 2022, paragraph 40, 61; and EDPB Statement 1/2024 on legislative developments regarding the Proposal for a Regulation laying down rules to prevent and combat child sexual abuse, Adopted on 13 February 2024.

[23] Article 3(h) DSA : '*illegal content' means any information that, in itself or in relation to an activity, including the sale of products or the provision of services, is not in compliance with Union law or the law of any Member State which is in compliance with Union law, irrespective of the precise subject matter or nature of that law*." Recital 12 DSA clarifies that "*the concept of 'illegal content' should be defined broadly to cover information relating to illegal content, products, services and activities. In particular, that concept should be understood to refer to information, irrespective of its form, that under the applicable law is either itself illegal, such as illegal hate speech or terrorist content and unlawful discriminatory content, or that the applicable rules render illegal in view of the fact that it relates to illegal activities. Illustrative examples include the sharing of images depicting child sexual abuse, the unlawful non-consensual sharing of private images, online stalking, the sale of non-compliant or counterfeit products, the sale of products or the provision of services in infringement of consumer protection law, the non-authorised use of copyright protected material, the illegal offer of accommodation services or the illegal sale of live animals*."

[24] And to the extent that the GDPR applies, for example, outside of purely personal or household activities of the recipients of the service (cf. Article 2(2)(c) GDPR).

[25] Article 5(1)(a) GDPR.

[26] Judgment of the Court of Justice of 11 December 2019 Asociaţia de Proprietari bloc M5A-ScaraA, C-708/1, ECLI:EU:C:2019:1064) paragraph 40; EDPB Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR, Version 1.0, Adopted on 8 October 2024, Chapter II.

[27] On the sharing of personal data with law enforcement agencies where intermediary service providers have identified potentially illegal content, see Judgment of the Court of Justice of 4 July 2023 Meta Platforms and

need to demonstrate that the legitimate interests pursued cannot reasonably be achieved just as effectively by other means less restrictive of the fundamental right to data protection.[28] Moreover, when carrying out the balancing test between the interests, rights and freedoms of data subjects, and the interest pursued by the controller, controllers should pay particular attention to whether the processing would be reasonably expected by data subjects,[29] and whether it concerns children.[30] Intermediary service providers (as controllers) should take all necessary steps to inform data subjects about the specific legitimate interest pursued by the processing,[31] and about the concrete measures envisaged by the controller to detect, identify and remove (or disable access to) illegal content in line with the data minimisation principle.

19. The second scenario covered by Article 7 DSA is one where intermediary service providers carry out processing, in good faith and in a diligent manner, **to comply with the requirements of Union law and national law in compliance with Union law**. Indeed, while Article 8 DSA prevents the EU or Member States from imposing on intermediary service providers general obligations to monitor the information they transmit or store or to seek facts or circumstances indicating illegal activity, there may be targeted legal obligations under EU or Member State law for such providers to detect and address illegal content.

> ***Example 1 – Identifying and taking down copyright-protected works in online content-sharing service***
>
> A company provides an intermediary service of which the main or one of the main purposes is to store and give the public access to a large amount of copyright-protected works or other protected subject matter uploaded by its users, which it organises and promotes for profit-making purposes. The company is thus qualified as an online content-sharing service provider under Directive (EU) 2019/790[32] (the 'Copyright Directive'). Under this Directive, the company is liable for unauthorised acts of communication to the public, including making available to the public, of copyright-protected

---

others, C-252/21, ECLI:EU:C:2023:537, which clarifies in paragraph 124 that "*as regards the objective referred to by the referring court, relating to the sharing of information with law-enforcement agencies in order to prevent, detect and prosecute criminal offences, it must be held that that objective is not capable, in principle, of constituting a legitimate interest pursued by the controller, within the meaning of point (f) of the first subparagraph of Article 6(1) of the GDPR. A private operator such as Meta Platforms Ireland cannot rely on such a legitimate interest, which is unrelated to its economic and commercial activity. Conversely, that objective may justify processing by such an operator where it is objectively necessary for compliance with a legal obligation to which that operator is subject*". See also EDPB Guidelines 01/2024 on processing of personal data based on Article 6(1)(f) GDPR, Version 1.0, paragraphs 131, 132, on circumstances in which a controller may rely on Art. 6(1)(f) GDPR to share information with law enforcement authorities in light of recital 50 GDPR.

[28] This includes compliance with the data minimisation principle under Article 5(1)(c) GDPR. See Judgment of the Court of Justice of 4 July 2023 Meta Platforms and others, C-252/21 ECLI:EU:C:2023:537, paragraphs 108 and 109.

[29] Judgment of the Court of Justice of 4 July 2023 Meta Platforms and others, C-252/21, ECLI:EU:C:2023:537, paragraph 112.

[30] Recital 38 GDPR. See also Judgment of the Court of Justice of 4 July 2023 Meta Platforms and others, C-252/21, ECLI:EU:C:2023:537, paragraphs 111 and 123.

[31] Article 13(1)(c) and (d) GDPR. See also Judgment of the Court of Justice of 4 July 2023 Meta Platforms and others, C-252/21, ECLI:EU:C:2023:537, paragraph 126.

[32] Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC, OJ L 130, 17.5.2019, p. 92–125.

works, unless they demonstrate that they have fulfilled a number of conditions. Among those conditions, companies are required to make, in accordance with high industry standards of professional diligence, best efforts to ensure the unavailability and re-upload prevention of specific works upon notification from rights-holders.[33] Although a company may need to process personal data to carry out such best efforts, such processing shall not lead to any identification of individual users nor the processing of personal data, except in accordance with Directive 2002/58/EC and Regulation (EU) 2016/679.[34]

20. Another example of a situation where an intermediary service provider could be obliged to process personal data pursuant to a requirement stemming from EU law would be where a data subject exercises their right to erasure under Article 17 GDPR because their personal data have been unlawfully processed (e.g., disseminated by a recipient of the service via an online platform without the data subject's consent or another legal basis). To comply with its obligation under Article 17 GDPR, the intermediary service provider may need to detect the allegedly illegal content and, after carefully considering whether an exception under Article 17(3) GDPR applies, decide whether the personal data should be erased or not.

21. To the extent that they require the processing of personal data, legal obligations may qualify as a legal basis for processing under Article 6(1)(c) GDPR. In line with the principle of accountability, intermediary service providers should determine the extent to which processing of personal data is necessary to comply with their existing legal obligations. In any case, such legal obligations should be clear and precise and their application should be foreseeable to persons subject to it, in accordance with the case-law of the CJEU.[35] Furthermore, the law must indicate in what circumstances and under which conditions a measure providing for the processing of personal data may be adopted, thereby ensuring that the interference is limited to what is strictly necessary.[36] 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.[37] If processing should be carried out in the context of compliance with an order issued by a competent authority to act against illegal content or to provide information about one or more specific individual recipients of the service, intermediary service providers are also required to check that the order complies with the requirements set out in Articles 9 or 10 of the DSA to justify processing under Article 6(1)(c) GDPR. The EDPB also notes that Recital 56 DSA clarifies that the DSA "*does not provide*

[33] Article 17(4) Copyright Directive. Recital 66 of the Directive further states that "*When assessing whether an online content-sharing service provider has made its best efforts in accordance with the high industry standards of professional diligence, account should be taken of whether the service provider has taken all the steps that would be taken by a diligent operator to achieve the result of preventing the availability of unauthorised works or other subject matter on its website, taking into account best industry practices and the effectiveness of the steps taken in light of all relevant factors and developments, as well as the principle of proportionality*".
[34] Article 17(9) Copyright Directive.
[35] Recital 41 GDPR. This complements the requirements of Article 7 and 8 of the Charter, as interpreted by the CJEU, according to which any interference must be provided for by law which is clear, precise and foreseeable.
[36] Judgment of the Court of Justice of 21 June 2022 Ligue des droits humains, C-817/19, ECLI:EU:C:2022:491, paragraph 117.
[37] Judgment of the Court of Justice of 9 November 2023 Gesamtverband Autoteile-Handel eV v Scania CV AB, C-319/22, ECLI:EU:C:2023:837, paragraphs 52 to 62.

the legal basis for profiling of recipients of the services with a view to the possible identification of criminal offences by providers of hosting services".

22. Depending on the level of automation involved in the processing, as well as the consequences it entails for data subjects, activities captured by Article 7 DSA may qualify as **decisions based solely on automated processing, including profiling, that are prohibited** under Article 22(1) GDPR.[38] On the one hand, it is possible that some decisions by intermediary service providers to remove allegedly illegal content could significantly affect recipients of the service whose content is removed.[39] On the other hand, it is particularly important to assess the degree of human involvement in a system involving automated processing of personal data for the detection and removal of illegal content: if there is no human involvement, if human involvement is not meaningful,[40] or if the human 'draws strongly' on the algorithmic recommendation generated by the system when deciding whether to remove the content,[41] the decision would still be considered as being based solely on automated processing under Article 22(1) GDPR. 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.[42] Furthermore, where Article 22(1) GDPR applies, intermediary service providers should avoid the processing of special categories of personal data, unless the conditions under Article 22(4) GDPR are fulfilled.

23. It is also important that intermediary service providers are **transparent** towards data subjects in relation to processing they carry out within the remit of Article 7 DSA. This involves providing them with all elements of information required under Articles 13 and 14 GDPR, in line with the conditions set

---

[38] Judgment of the Court of Justice of 7 December 2023 OQ v Land Hessen, C-634/21, ECLI:EU:C:2023:957, paragraph 52: "*Article 22(1) of the GDPR confers on the data subject the 'right' not to be the subject of a decision solely based on automated processing, including profiling. That provision lays down a prohibition in principle, the infringement of which does not need to be invoked individually by such a person*". See also Article 29 Data Protection Working Party Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (WP251rev.01), as last Revised and Adopted on 6 February 2018.

[39] Article 29 Data Protection Working Party Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (WP251rev.01), as last Revised and Adopted on 6 February 2018, page 21: "*For data processing to significantly affect someone the effects of the processing must be sufficiently great or important to be worthy of attention. In other words, the decision must have the potential to:*

- *significantly affect the circumstances, behaviour or choices of the individuals concerned;*
- *have a prolonged or permanent impact on the data subject; or*
- *at its most extreme, lead to the exclusion or discrimination of individuals*".

[40] Article 29 Data Protection Working Party Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (WP251rev.01), as last Revised and Adopted on 6 February 2018, page 21: "*The controller cannot avoid the Article 22 provisions by fabricating human involvement. For example, if someone routinely applies automatically generated profiles to individuals without any actual influence on the result, this would still be a decision based solely on automated processing. To qualify as human involvement, the controller must ensure that any oversight of the decision is meaningful, rather than just a token gesture. It should be carried out by someone who has the authority and competence to change the decision*".

[41] Judgment of the Court of Justice of 7 December 2023 OQ v Land Hessen, C-634/21, ECLI:EU:C:2023:957, paragraphs 62 and 73.

[42] Article 29 Data Protection Working Party Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (WP251rev.01), as last Revised and Adopted on 6 February 2018, pages 23 and 24.

forth in Article 12 GDPR.[43] If the processing qualifies as automated decision-making under Article 22(1) GDPR, the controller must inform data subjects that they are engaging in this type of activity, provide meaningful information about the logic involved in the decision-making, and explain the significance and envisaged consequences of the processing.[44] Articles 14(1) and 15(1)(c) and (e) DSA include additional transparency requirements for intermediary service providers concerning their policies, procedures, measures and tools used for the purpose of content moderation - including algorithmic decision-making and human review -, as well as disclosing possible error rates of the automated means used for content moderation purposes, and any safeguards applied. Further transparency requirements derive from Article 17 DSA, which may require providers of hosting services to provide a clear and specific statement of reasons to any affected recipients of the service for any of the restrictions under Article 17(1) DSA imposed on the grounds that the information provided by the recipient of the service is illegal content or incompatible with the terms and conditions of the service.[45] In particular, according to Article 17(3)(b) DSA, the statement of reasons must contain, inter alia, information on whether the decision was taken pursuant to a voluntary own-initiative investigation.

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.

2.2 Processing of personal data in notice and action mechanisms and in internal complaint-handling systems (Articles 16, 17, 20, and 23)

2.2.1 Processing activities involved by the notice and action mechanisms (Articles 16 and 17 DSA)

25. In order to tackle illegal content online, the DSA envisages an obligation for any providers of hosting services to put in place mechanisms that will help individuals or entities report illegal content by means of notifications. To this end, Article 16 DSA envisages that any providers of hosting services, regardless of their size[47] and including online platforms, have an obligation to put in place 'notice and action'

---

[43] See, for more detailed guidance, Article 29 Working Party Guidelines on transparency under Regulation 2016/679 (WP260 rev.01), as last Revised and Adopted on 11 April 2018.

[44] Article 29 Data Protection Working Party Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (WP251rev.01), as last Revised and Adopted on 6 February 2018, page 24-26.

[45] Cf. paragraph 34.

[46] Article 29 Data Protection Working Party Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (WP 248), Adopted on 4 April 2017, pages 7-9.

[47] Recital (50) DSA provides examples for the type of providers to which the obligation is addressed. It also refers to "*file storage and sharing services, web hosting services, advertising servers and paste bins, in so far as they qualify as hosting services covered*" by the DSA.

mechanisms allowing individuals or entities to notify, by electronic means, the presence of specific items of information that they consider to be illegal content. Upon receipt of such notification the hosting service provider can decide whether or not it agrees with that assessment and decide to take an action (e.g. restriction on visibility such as removal of content, demoting content or suspension, termination or other restriction of monetary payments, etc.).[48]

26. These mechanisms can be triggered, according to Article 22 DSA, also by trusted flaggers, i.e. "entities, and not individuals, that have demonstrated, among other things, that they have particular expertise and competence in tackling illegal content and that they work in a diligent, accurate and objective manner"[49].

27. These 'notice and action' systems, in particular when initiated by an individual, may imply the processing of personal data of the individual submitting the notice (the 'notifier') and of the affected recipients of the service, when they are also individuals. They may also trigger the processing of personal data of third parties if, in order to identify the illegal content, the notice or the identified content contain personal data of third parties. In such cases therefore the hosting service providers will qualify as controllers and will have to respect and process personal data in accordance with the GDPR.

28. With regard to personal data of the 'notifier'[50], with a view to facilitating the submission of sufficiently precise and adequately substantiated notices, Article 16(2) DSA envisages that the hosting providers shall 'enable' and 'facilitate' the submission by electronic means, among the other information related to the illegal content, of the name and email address of the notifier. This information should not be collected where it is considered to involve one of the offences referred to in Articles 3 to 7 of the directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography ('CSAM directive').

29. In light of the provisions contained in the DSA and where available in the notice submitted by the notifier, the hosting provider will be entitled, therefore, to process the name and email address of the notifier in order to provide them, without undue delay, with a confirmation of receipt of the notice, its decision in relation to the information 'notified' and information in relation to the means of redress against this decision.[51] By the same token, the name and email address should be used, where available, to send a notice to the notifier to inform them of cases where the hosting providers cannot, for technical or operational reasons, remove the specific item of information.[52] In addition, and 'only where strictly necessary', personal data of the notifier should be included in the statement of reasons to be provided to the affected recipients of the service.[53]

30. In setting out and implementing the rules for the functioning of the 'notice and action' system, there is therefore a need to provide robust safeguards to protect the right to personal data of all the parties involved, including the notifier.[54] In this respect, the EDPB would recall that personal data should be

---

[48] See Article 17(1) DSA.

[49] Recital 61 DSA. According to Article 22(3) DSA, the trusted flaggers shall publish, at least once a year, detailed reports on notices submitted in accordance with Article 16 which should not contain personal data.

[50] The notifier is the individual or entity who notifies a provider of a hosting service about allegedly illegal content.

[51] See Article 16(4) and 16(5) DSA.

[52] Recital 51 DSA.

[53] Article 17(3)(b) DSA.

[54] Recital 52 DSA recommends, in this regard, that "[t]*he rules on such notice and action mechanisms should be harmonised at Union level, so as to provide for the timely, diligent and non-arbitrary processing of notices on the basis of rules that are uniform, transparent and clear and that provide for robust safeguards to protect the right*

limited to those necessary for the specific purposes referred to in the DSA relevant provisions. Hence, for example, providers should generally not ask for notifiers' additional personal data than those referred to in Article 16(2) DSA. This considering that, when additional identification data are deemed to be necessary, the DSA expressly mentions them[55] 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).

31. By the same token, according to the principle of accountability, the controller should define the cases where it would be necessary and proportionate to reveal, pursuant to Article 17(3)(b) DSA, the notifier's identity to the affected recipients of the service. Recital 54 already clarifies that this could happen when "this information is necessary to identify the illegality of the content" and e.g. refers to cases of infringements of intellectual property rights. In such cases, it should be ensured that only strictly necessary personal data of the notifier is communicated to the affected recipient of the service and the data subject, i.e. the notifier, should be duly informed, according to Article 13 GDPR, that such processing activity can take place.

32. Article 16(6) DSA envisages that hosting providers may make use of automated means for processing any notices that they receive under this mechanism or for the decision-making process and prescribes, in such cases, to provide the individual or entity that submitted the notice with information on such use. This should be in addition to the information provided under Article 13 GDPR, including in what concerns automated decision-making, if applicable.

33. The EDPB welcomes that this provision increases transparency towards notifiers as data subjects and recalls that in cases where such removal could fall under the scope of Article 22 GDPR, this provision imposes strict conditions on decisions based solely on automated processing, including profiling, that produce legal effects, or similarly significantly affect the concerned individual. In particular, it is important to recall that where a decision based solely on automated processing is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests - as it is the case with the notice and action mechanism envisaged by the DSA -,[56] such automated decisions shall not be based on special categories of personal data, unless the data subject has given explicit consent or processing is necessary for reasons of substantial public interest in accordance to Article 9(2)(a) or (g) GDPR.[57]

34. Article 17 DSA requires the provider of hosting services to provide a clear and specific statement of reasons to the affected recipients of the service for any decision to remove or disable access to specific items of information they provided both in case where the information provided by the recipient of the service is illegal content or where it is incompatible with their terms and conditions of the service. This obligation will apply only where the relevant electronic contact details are known to the provider

---

and legitimate interests of all affected parties, in particular their fundamental rights guaranteed by the Charter, irrespective of the Member State in which those parties are established or reside and of the field of law at issue".

[55] See, for example, Article 30 DSA on traceability of traders, that requires providers of online platforms to obtain the name, address, telephone number and email address of the trader and a copy of their identification document or any other electronic identification.

[56] Article 22(2)(b) GDPR.

[57] Article 22(4) GDPR.

and it will not apply when the action is taken '[u]pon the receipt of an order to act against one or more specific items of illegal content, issued by the relevant national judicial or administrative authorities' according to Article 9 DSA.[58]

35. Article 17(3)(c) DSA, by referring to the obligation to inform the affected recipients about the use of automated means in taking the decision, implies the possibility for providers of hosting services to make use of automated means to process or make decisions about the notices received.

36. In this respect, the EDPB recalls that, as already considered by the EDPS in its Opinion 1/2021 on the Proposal for a Digital Services Act,[59] Article 22 GDPR imposes strict conditions on decisions based solely on automated processing, including profiling, leading to decisions that may produce legal effects, or similarly significantly affect the individual concerned. In particular, Article 22(2)(b) GDPR envisages that a decision can be based solely on automated processing where it is authorised by Union or Member State law which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests[60].

37. Regardless of whether the action taken by the hosting provider qualifies as automated decision making under Article 22 GDPR, Article 17(3) DSA imposes on the hosting providers the obligation to provide the data subjects (i.e. the affected recipients when they are individuals) with some specific information and, among them the envisaged action to be taken, the facts and circumstances relied on in taking the decision, the use of automated means in taking the decision, but also on whether the decision was taken in respect of content detected or identified using automated means, on the legal ground relied on and on the reasons why the information is considered to be illegal content on that ground and on the possibilities for redress available to the recipient of the service in respect of the decision.

2.2.2 Processing of personal data of the affected recipient by providers of online platforms for handling of complaint and combatting misuse (Articles 20 and 23)

38. In the framework of the activities aimed at combating the illegal content, Section 3 of Chapter III DSA imposes only on providers of online platforms some additional obligations which may involve the processing of personal data.

39. Pursuant to Article 20 DSA, both the affected recipients of decisions concerning the illegality of content or its incompatibility with the online platforms' terms and conditions and the individuals (or entities) that have submitted a notice are entitled to lodge a complaint in order to, respectively, contest a decision that negatively affects them or to contest allegedly inadequate action taken on the basis of the notice submitted.[61] The EDPB welcomes that, in both cases, the DSA envisages that the providers of online platform shall ensure that the decisions referred to in Article 20 are taken under the supervision of appropriately qualified staff, and not solely on the basis of automated means.[62] The EDPB recalls that, also in this case, the providers of online platforms will act as controllers of the personal data involved and should therefore respect the relevant GDPR provisions. In particular, it is worth noting that the complaint mechanism under Article 20 DSA is without prejudice to the rights and remedies

[58] Article 17(5) DSA.
[59] EDPS Opinion 1/2021 on the Proposal for a Digital Services Act, 10 February 2021 paragraph 42.
[60] See also Judgment of the Court of Justice of 7 December 2023 OQ v Land Hessen, C-634/21, ECLI:EU:C:2023:957, paragraphs 65- 66.
[61] Article 20(1) DSA.
[62] Article 20(6) DSA.

available to data subjects pursuant to the GDPR vis-à-vis providers of online platforms acting as controllers.

40. Besides, considering that "misuse of online platforms by frequently providing manifestly illegal content or by frequently submitting manifestly unfounded notices or complaints […] undermines trust and harms the rights and legitimate interests of the parties concerned",[63] Article 23 DSA allows online platforms to suspend their relevant activities in respect of the person engaged in abusive behaviour, i.e. recipients that frequently provide manifestly illegal content[64] and notifiers or complainants that frequently submit manifestly unfounded notices or complaints[65].

41. While envisaging safeguards against the misuse of online platforms, the DSA also envisages that such safeguards should be "appropriate, proportionate and effective" and need "to respect the rights and legitimate interests of all parties involved, including the applicable fundamental rights and freedoms as enshrined in the Charter".[66] In this regard, the EDPB welcomes the safeguards the DSA already identifies,[67] as they will allow avoiding the adoption of automated decisions in such cases and recalls to the providers of online platforms that, when identifying the measures for combating misuse and setting out in their terms and conditions their policy in this regard, they should take into account the need to ensure the respect of all the data protection principles set forth in Article 5 GDPR and, in particular, the minimisation, accuracy, transparency and data retention principles.

42. It is likely that decisions by providers of online platforms to suspend their relevant activities in respect of persons they consider to be engaged in abusive behaviour may significantly affect their rights. For this reason, the respect of the accuracy principle is particularly relevant in order to avoid suspensions from the use of the notice and action mechanisms based on the processing of inaccurate personal data. It is also important that online platform providers are transparent towards data subjects in relation 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. In addition, the respect of data minimisation and data retention principles should be carefully considered so as to ensure that only personal data that will be strictly necessary to the purpose of avoiding the submission of manifestly unfounded notices or complaints are processed and only for the timeframe that is necessary for the envisaged purposes, taking into account that Article 23 allows only for suspension issued 'for a reasonable period of time'. Finally, the EDPB highlights that the suspension of an account is without prejudice to the data subject rights under the GDPR, including the right to data portability in relation to personal data that will still be processed by the provider of online platform during the suspension of the service.

2.3 Deceptive design patterns (Article 25)

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. The EDPB Guidelines on deceptive design patterns highlight that such patterns

[63] Recital 63 DSA.
[64] Article 23(1) DSA.
[65] Article 23(2) DSA.
[66] Recital 63 DSA.
[67] According to Article 23(1) DSA, providers of online platform shall suspend their services only for a reasonable period of time and after having issued a prior warning containing the reasons for the possible suspension and the means of redress against this decision. In addition, Article 23(3) DSA clarifies that any decision of suspension according to Article 23 DSA should be taken "on a case-by-case basis".

"attempt to influence users into making unintended, unwilling and potentially harmful decisions, often toward a decision that is against the users' best interests and in favour of the [online] platforms interests, regarding the processing of their personal data. Deceptive design patterns aim to influence users' behaviour and can hinder their ability to effectively protect their personal data and make conscious choices".[68] According to Article 25(2) DSA, the prohibition in Article 25(1) DSA shall not apply to practices covered by the GDPR or by Directive 2005/29/EC (Unfair Commercial Practices Directive, UCPD). Examples of deceptive design patterns can be found in Recital 67 DSA, the EDPB Guidelines 3/2022 on deceptive design patterns in social media platform interfaces,[69] and the EU Commission Notice (2021/C 526/01) on the Unfair Commercial Practices Directive (UCPD).[70] The Consumer Protection and Cooperation Network[71] (CPC) also carried out a sweep on dark patterns that is of relevance for the application of EU consumer protection law to deceptive design patterns.[72] Insofar as Article 25(1) DSA is applicable, there is an example in Recital 67 DSA of what should not constitute a deceptive design, namely "[l]egitimate practices, for example in advertising, that are in compliance with Union law should not in themselves be regarded as constituting [deceptive design] patterns".

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.[73] Key elements to consider when assessing whether a deceptive design pattern is covered by the GDPR are whether personal data is being processed and whether the data subject's behaviour that the pattern is influencing relates to the processing of personal data.[74] For example, patterns that try to push all recipients of a service to buy a product by (emotional) steering, e.g., "There are only a few products left in stock", may not be covered by the GDPR. However, if the recipient of the service is manipulated into providing (additional) personal data, for example, "There are only a few products left in stock. Enter your email address now and make a reservation", or provide more personal data than they would have otherwise, then the pattern is subject to the GDPR. Additionally, if the recipient of the service is a legal person, e.g., a business user, the GDPR does not apply, insofar as no personal data relating to a natural person would be processed.[75] In any event, Article 25(1) DSA applies if the deceptive design pattern is not covered by the UCPD or the GDPR, and provides a clear general prohibition of deceptive design patterns for providers of online platforms.

45. It should be mentioned that the processing of personal data pursuant to Article 5(1)(a) GDPR must take place lawfully, fairly and in a transparent manner in relation to the data subject and therefore the use of deceptive design patterns covered by the GDPR is generally unlawful. The EDPB recalls that

---

[68] EDPB Guidelines 3/2022 on Deceptive design patterns in social media platform interfaces: how to recognise and avoid them, version 2.0, Adopted on 14 February 2023, page 3.
[69] EDPB Guidelines 3/2022 on Deceptive design patterns in social media platform interfaces: how to recognise and avoid them, version 2.0, Adopted on 14 February 2023.
[70] EU Commission Notice (2021/C 526/01) offers Guidance on the interpretation and application of the UCPD, including on "dark patterns" in its Section 4.2.7.
[71] CPC Network, https://commission.europa.eu/live-work-travel-eu/consumer-rights-and-complaints/enforcement-consumer-protection/consumer-protection-cooperation-network_en.
[72] CPC network, https://commission.europa.eu/live-work-travel-eu/consumer-rights-and-complaints/enforcement-consumer-protection/sweeps_en#ref-2022--sweep-on-dark-patterns.
[73] EDPB Guidelines 3/2022 on Deceptive design patterns in social media platform interfaces: how to recognise and avoid them, version 2.0, Adopted on 14 February 2023, paragraph 4.
[74] Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, WP 136, Adopted on 20 June 2007, page 10; cf. Judgment of the Court of Justice of 20 December 2017 Peter Nowak v Data Protection Commissioner, C-434/16, ECLI:EU:C:2017:994, , paragraph 35.
[75] Article 4(1) GDPR.

"*fairness is an overarching principle which requires that personal data shall not be processed in a way that is detrimental, discriminatory, unexpected or misleading to the data subject*", which is often the case when a controller deploys deceptive design patterns.[76]

46. A special case of deceptive design patterns are design patterns, that "may cause addictive behaviour" or "may stimulate behavioural addictions of recipients of the service", and are identified in Recitals 81 and 83 DSA as possible sources of systemic risks.[77] These patterns can rely on design features, attributes or practices that incentivise users to spend much more time using online platforms. These patterns are usually designed to deceive, manipulate or materially distort or impair the ability of users to make free and informed decisions.[78] The use of these deceptive design patterns may require personal data as input, involve the collection or generation of new personal data and profiles, or influence user behaviour and decision-making in the context of personal data processing.

47. Common examples of deceptive design patterns that may cause addictive behaviour include infinite scrolling, infinite streaming, autoplay, periodic rewards, status or reputation improvements, collection completion, gamification, countdown timers, among others.[79] Examples of such patterns are also described in the EDPB Guidelines on Deceptive design patterns in social media platform interfaces and aim, inter alia, to "[influence] the emotional state of users in such a way [that] is likely to lead them to make an action that works against their data protection interests".[80]

2.4 Advertising transparency and prohibition of presenting advertisements based on profiling using special categories of data (Article 26)

48. Article 26 DSA lays down transparency rules for providers of online platforms regarding advertising and prohibits providers of online platforms from presenting advertisements to recipients based on profiling using special categories of data referred to in Article 9(1) GDPR.

49. Recital 68 of the DSA clarifies that the requirements under Article 26 DSA are without prejudice to the GDPR, "in particular those regarding the right to object, automated individual decision-making, including profiling, and specifically the need to obtain consent of the data subject prior to the processing of personal data for targeted advertising". It is also without prejudice to the provisions in the ePrivacy Directive,"in particular those regarding the storage of information in terminal equipment and the access to information stored therein".

---

[76] EDPB Guidelines 3/2022 on Deceptive design patterns in social media platform interfaces: how to recognise and avoid them, version 2.0, Adopted on 14 February 2023, in particular paragraphs 9 ff.; EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, version 2.0, Adopted on 20 October 2020, in particular page 16.

[77] "'[M]anipulative design', 'addictive design' or 'behavioural design' of online services describe features that lead to behaviour-related risks and harms, including forms of digital addiction, such as, 'excessive or harmful internet use', 'smartphone addiction', 'technological or internet addiction', 'social media addiction'", European Parliament resolution of 12 December 2023 on addictive design of online services and consumer protection in the EU single market (2023/2043(INI)), paragraph A; Cf. the recent Study to support the Fitness Check of EU consumer law on digital fairness and the report on the application of the Modernisation Directive (EU) 2019/2161.

[78] Ibid.

[79] Ibid.

[80] EDPB Guidelines 3/2022 on Deceptive design patterns in social media platform interfaces: how to recognise and avoid them, version 2.0, Adopted on 14 February 2023, in particular section 4.3.

2.4.1 General advertising transparency obligations

50. Articles 13 and 14 GDPR define the information to be provided to the data subjects when their personal data are processed, and the modalities for doing so. These general rules are applicable to any data processing, including processing that could occur in the context of advertising on online platforms.

51. Article 26(1) DSA lays down transparency rules for providers of online platforms specifically regarding advertising. This provision states that information regarding each specific advertisement should be provided to the recipients of the service in real time. Additionally, meaningful information regarding the main parameters used to determine the recipient to whom the advertisement is presented and, where applicable, information about how to change those parameters as specified in Article 26(1)(d) DSA must be directly accessible from the advertisement.

52. It means that the elements of information mentioned in Article 26 DSA should be provided in real time, directly accessible from the advertisement, while information related to transparency obligations as set out in Articles 13 and 14 GDPR could be presented through the means of a privacy policy (e.g., one click away).

53. It also means that information required under Article 26 DSA would be provided after a processing of personal data may have occurred.

54. This is an important difference between Article 26 DSA and the transparency requirements under the GDPR, since the latter provides that in case of personal data collected directly from the data subject, information shall be provided at the time when personal data are obtained, as set out in Article 13(1) and 13(2) GDPR, before the processing takes place.

55. The transparency requirements under Article 26 DSA apply irrespectively of the legal basis for processing under Article 6(1) GDPR by the provider of the online platform.

56. Moreover, if processing for advertising purposes is based on consent (Article 6(1)(a) GDPR), certain information regarding processing (including profiling) must already be provided to the individual before consent is collected. Additional information pursuant to Article 26(1)DSA would later be directly and easily accessible to the recipient from the advertisement.

2.4.2 Legal framework on automated individual decision-making and profiling

57. According to Article 26(1)(d) DSA, "*providers of online platforms that present advertisements on their online interfaces shall ensure that, for each specific advertisement presented to each individual recipient, the recipients of the service are able to identify, in a clear, concise and unambiguous manner and in real time* […] *meaningful information directly and easily accessible from the advertisement about the main parameters used to determine the recipient to whom the advertisement is presented and, where applicable, about how to change those parameters*".

58. In its Recital 68, the DSA indicates that "*Such explanations should include information on the method used for presenting the advertisement, for example whether it is contextual or other type of advertising, and, where applicable, the main profiling criteria used; it should also inform the recipient about any means available for them to change such criteria*".

59. Article 4(4) GDPR defines profiling as "*any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability behaviours, location or movements*".

60. Indeed, providers of online platforms and other actors that gather information on preferences of users of an online platform in order to enable advertisements to be presented to them accordingly, often conduct profiling under the definition set out in Article 4(4) GDPR.[81]

61. However, Article 26(1) DSA also applies to forms of advertising that do not involve profiling and that may involve the processing of less (or no) personal data, e.g. general advertising.

62. The provisions in Article 26(1) DSA on advertising transparency also 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,[82] if the profiling in question leads to a decision that produces legal effects or similarly significantly affects data subjects.[83] To assess whether an automated decision to present a specific advertisement to an individual produces legal effects or similarly significantly affects him or her, several (non-exhaustive) characteristics of the personal data processing activity (including at the level of each individual advertisement delivery) should be taken into account, including the intrusiveness of the profiling process, 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.[84]

63. According to Article 22(1) GDPR, the data subject has "*the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her*".

64. However, such processing can be lawful if it relies on specific legal bases as defined in Article 22(2) GDPR necessary for the performance of a contract, authorised by Union or Member State law or based on the data subject's explicit consent.

65. Whether or not the data has been obtained directly or indirectly, the GDPR mandates that the data subject shall be properly informed, according to Articles 13 and 14 GDPR, of "*the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing*". Recital 71 GDPR also indicates that processing within the scope of Article 22 GDPR "*should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision*

---

[81] See also EDPB Guidelines 8/2020 on the targeting of social media users, version 2.0, Adopted on 13 April 2021.
[82] See Article 29 Data protection working party, Guidelines on Automated individual decision-making and Profilingfor the purposes of Regulation 2016/679, Adopted on 3 October 2017, As last Revised and Adopted on 6 February 2018, WP251rev.01, page 22.
[83] Article 26(1) DSA requires providers of online platforms to provide transparency about the main parameters used to determine the recipient to whom the advertisement is presented and, where applicable, how to change those parameters. The provision does not specifically require providers of online platforms to provide information about whether profiling was used in determining the recipient to whom the advertisement was shown, while such information may need to be provided under Article 13(2)(f) or 14(2)(g) GDPR if the profiling falls under Article 22(1) GDPR.
[84] EDPB Guidelines 8/2020 on the targeting of social media users, version 2.0, Adopted on 13 April 2021, example 8 in page 24, paragraphs 85-88. See also Article 29 Data protection working party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, Adopted on 3 October 2017, As last Revised and Adopted on 6 February 2018, WP251rev.01, pages 21 and 22.

(…)".[85] Moreover, Recital 60 GDPR states that "*the data subject should be informed of the existence of profiling and the consequences of such profiling*"[86] even where profiling does not fall within the scope of Article 22 GDPR.

66. Some of the elements or parts of the elements mentioned in Article 26 DSA should therefore already be provided to the data subject under the GDPR especially where Article 22 GDPR applies, in particular regarding the main parameters of the profiling.[87]

67. Therefore, the DSA and the GDPR both include transparency obligations that are relevant to the delivery of advertisements on online platforms. The DSA lays down additional obligations, as it specifies the manner in which the relevant information must be provided and the expected level of information and control, for instance providing the main parameters for determining that a specific advertisement is presented to the recipient and providing information on possibilities to change said parameters, where such possibilities exist.

68. In any event, pursuant to Article 5(1)(b) GDPR, personal data shall be collected for specified, explicit and legitimate purposes, whether this processing leads to the presentation of an advertisement or not.

69. Processing of personal data must rely on a valid legal basis according to GDPR in order to be lawful, regardless of whether this processing constitutes profiling, leads to the presentation of an advertisement or serves another purpose.

70. For instance, if such processing relies on consent as set out in Article 6(1)(a) GDPR and Article 5(3) of ePrivacy directive, consent must fulfil all the criteria laid out in Articles 4(11) and 7 GDPR in order to be considered valid.[88] In particular, data subjects must be able to withdraw their consent at any moment, as easily as it was to give their consent, and shall also be informed about this possibility.

71. If such processing relies on legitimate interests,[89] data subjects have an unconditional right to object to processing for "direct marketing" purposes under Article 21(3) GDPR. This includes processing carried out for showing targeted advertisements (presenting a message with a commercial purpose directly and individually to an end user),[90] provided that these targeted advertisements are not already prohibited under Article 26(3) DSA.

---

[85] See also See Article 29 Data protection working party, Guidelines on Automated individual decision-making and Profilingfor the purposes of Regulation 2016/679, Adopted on 3 October 2017, As last Revised and Adopted on 6 February 2018, WP251rev.01, Chapter IV (section E), page 24.

[86] See also See Article 29 Data protection working party, Guidelines on Automated individual decision-making and Profilingfor the purposes of Regulation 2016/679, Adopted on 3 October 2017, As last Revised and Adopted on 6 February 2018, WP251rev.01, Chapter III (section D), page 16.

[87] See Article 29 Data protection working party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, Adopted on 3 October 2017, As last Revised and Adopted on 6 February 2018, WP251 rev.01, page 25 on "Meaningful information about the 'logic involved'". See also Judgment of the Court of Justice of 27 February 2025 Dun & Bradstreet Austria GmbH, C-203/22, ECLI:EU:C:2025:117, , paragraphs 60 and 61.

[88] EDPB Guidelines 05/2020 on consent under Regulation 2016/679, version 1.1, Adopted on 4 May 2020.

[89] See Judgment of the Court of Justice of 4 July 2023 Meta Platforms and others, C-252/21, ECLI:EU:C:2023:537, paragraph 86 and following regarding legitimate interests in the context of advertising.

[90] See Judgment of the Court of Justice of 25 November 2021 StWL Städtische Werke Lauf a.d. Pegnitz GmbH v eprimo GmbH, C-102/20, ECLI:EU:C:2021:954, paragraph 47. In paragraph 50 of the judgment, the CJEU also mentioned that it is irrelevant whether the advertising at issue is addressed to a predetermined and individually identified recipient or is sent on a mass, random basis to multiple recipients.

2.4.3 Legal framework on profiling using special categories of data

72. Processing of special categories of data,[91] including profiling based on these data, are subject to a specific legal regime as set out in Article 9 GDPR. Processing of such special categories of data is prohibited in principle, unless it relies on specific derogations, as set out in Article 9(2) GPDR. The scope of the special categories of data under Article 9(1) GDPR is very broad. In particular, it may include data derived or inferred from profiling activity[92] or indirect disclosure of such data[93]. Moreover, it does not matter if the information revealed by the processing operation in question is correct and if the controller is acting with the aim of obtaining information that falls in that category.[94]

73. Moreover, automated individual decision-making within the scope of Article 22 GDPR shall not be based on special categories of personal data referred to in Article 9(1) GDPR unless such processing relies on the explicit consent of the data subject (Article 9(2)(a)) GDPR or is necessary for reasons of substantial public interest (Article 9(2)(g) GDPR) pursuant to Article 22(4) GDPR.

74. However, according to Article 26(3) DSA, "*Providers of online platforms shall not present advertisements to recipients of the service based on profiling as defined in Article 4, point (4), of Regulation (EU) 2016/679 using special categories of personal data referred to in Article 9(1) of Regulation (EU) 2016/679*".

75. This means that the GDPR requires specific derogations regarding profiling by online platforms using special categories of data for advertising purposes. On the other side, the DSA prohibits the presentation of any advertising based on profiling using such special categories of personal data by providers of online platforms to recipients of the service, regardless of whether this profiling is carried out by providers of online platforms or by others.

Example 2 – Profiling based on special categories of data

A company uses inferred religious beliefs from geolocation (e. g. visiting places of worship) or shopping habits (e. g. purchase of specific food products) to predict lifestyle and shopping patterns and then presents an advertisement based on those predictions.

76. These special rules laid down by the DSA complement the rules laid down in Article 9(2) GDPR and Article 22(4) GDPR when they apply. The presentation of advertisements based on profiling using special categories of personal data by providers of online platforms to recipients of the service is prohibited by the DSA even in situations where the provider of an online platform or another entity would rely on an appropriate legal basis under Article 6(1) GDPR and an appropriate derogation under Article 9(2) GDPR for this processing.

[91] Article 9(1) GDPR: "*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*".

[92] Judgment of the Court of Justice of 4 July 2023 Meta Platforms and others, C-252/21, ECLI:EU:C:2023:537, paragraph 73.

[93] Judgment of the Court of Justice of 1 August 2022 OT and Lithuania, C-184/20, ECLI:EU:C:2022:601.

[94] Judgment of the Court of Justice of 4 July 2023 Meta Platforms and others, C-252/21, ECLI:EU:C:2023:537, paragraph 69.

2.4.4 Security and confidentiality of data resulting from advertising transparency obligations

77. Article 26(1)(d) DSA states that information must be provided about the main parameters used to determine the recipient to whom each advertisement is presented. As per Recital 68 of the DSA, "*recipients of the service should have information directly accessible from the online interface where the advertisement is presented, on the main parameters used for determining that a specific advertisement is presented to them, providing meaningful explanations of the logic used to that end, including when this is based on profiling*". In practice, that information likely often constitutes personal information as it can reveal alleged user preferences and prior navigation.

78. As recalled in Recital 107 DSA, "*The provision of online advertising generally involves several actors, including intermediary services that connect publishers of advertisements with advertisers*". For the relevant information to reach the recipient of the service, those intermediaries need to facilitate the transmission of information. Appropriate technical and organisational measures need to be implemented to ensure that the presentation of that information and the ability to change parameters – where such possibilities exist – does not allow any intermediary to access or collect any additional information about the recipient of the service. The associated processing should respect the obligation provided by Article 32 GDPR, as well as data minimisation according to Article 5(1)(c) GDPR, and data protection by design and default under Article 25 GDPR. Compliance with the transparency obligations set out in Article 26 DSA should not entail further sharing of personal data with intermediaries: access or collection of information regarding the recipient of the service through intermediary companies requires an appropriate legal basis under Article 6 GDPR and must respect the principles laid out in Article 5 GDPR.

79. Additionally, providers of intermediary services should, where possible and without leading to an increased collection of personal data, take appropriate steps to ensure that the information is provided to the one recipient of the service that is subject to such profiling.

2.5 Recommender systems (Articles 27 and 38)

80. A "recommender system" as defined by Article 3(s) DSA is a partially or fully automated system used by online platforms to present specific content to users of the platform with a certain relative order or prominence. Online search engines may use recommender systems when proposing search results to users as well.[95] These systems are widespread in today's online platforms because of their usefulness in facilitating and optimising access to information for the recipients of the service, and the DSA recognizes their significant role in the amplification and viral dissemination of content as well as the stimulation of online behaviour.[96] The DSA also introduces specific safeguards in Articles 27 and 38 DSA to empower users.

81. Providers of online platforms whose services have a large catalogue of content often want to propose specific content first or prominently to their users, usually at the landing page of their web site or through their app feed or other features of their service where they present content to users, because of an otherwise potentially overwhelming number of content items that can discourage users from continuing their use of the service. The selection and the order by which content is presented is usually the result of some criteria defined by the provider of the online platform and constitutes a recommendation among all the content the platform can disseminate. The recommendation activity involves filtering, ranking or applying other types of prioritisation logic to content, often personalised, with the aim of presenting what is most likely to interest users first, or with a view to enhance the quality or

[95] See Article 3(s) and (j) DSA.
[96] See Recital 70 DSA.

diversity of the content presented to users. Although recommender systems may involve the processing of personal data, there are circumstances where this may not be the case. For example, an e-commerce web site provider could decide to propose to clients landing on its home page bestselling products first. In such a case, the recommendation is made without awareness of specific characteristics of the user visiting the service, and the underlying recommendation process does not involve any processing of personal data.

82. However, real world scenarios increasingly involve automated personal data processing with the aim to personalise and make more efficient the content presentation: when selecting items to be displayed to users, recommender systems' algorithms usually process data about their behaviour, and can also build on data about the behaviour of other users to make a prediction on what items would more likely attract and lead users to engage with the content.[97]

83. While personal data processing enables providers to embed into their online platforms efficient and precise recommender systems, it is important to underline that those systems also entail risks for individuals subject to them.[98] Some of these risks relate to 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 to the processing of special categories of data or data of highly personal nature or data of vulnerable data subjects.[99]

84. According to the GDPR, behavioural analysis for prediction purposes constitutes a profiling activity as it involves "the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's (…) personal preferences, interests, (…) behaviour"[100]. Personal data processing in the context of recommender systems is subject to the GDPR, including the principles of lawfulness, fairness and transparency, purpose limitation, and accuracy.[101] The requirements to secure an appropriate legal basis under Article 6(1) GDPR to profile data subjects in that context and (if applicable) a derogation under Article 9(2) GDPR if special categories of data are involved have particular importance. It should also be highlighted that it cannot be excluded that the presentation of specific content to users of an online platform via a recommender system would be a 'decision' in the meaning of Article 22(1) GDPR, i.e. a decision which significantly affects the data subject. In this context, a decision should be seen as "*a broad concept which can include a number of acts capable of affecting the data subject in many ways*"[102]. Having this in mind, it may not be ruled out that, in some cases, the processing of personal data carried out in the context of presenting specific content to users of an online platform via a recommender system may correspond

---

[97] This is called "collaborative filtering". See Schafer, J.B., Frankowski, D., Herlocker, J., Sen, S. (2007). Collaborative Filtering Recommender Systems. In: Brusilovsky, P., Kobsa, A., Nejdl, W. (eds) The Adaptive Web. Lecture Notes in Computer Science, vol 4321. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-72079-9_9.

[98] Recital 70 DSA.

[99] Cf. Article 29 Data Protection Working Party Guidelines on Data Protection Impact Assessment (DPIA) and determining the criteria whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP 248 rev.01, 4 October 2017, p. 9 ff.

[100] Article 4(4) GDPR.

[101] See Article 4(4) and Article 5 GDPR.

[102] Opinion of Advocate General Pikamäe in Case C-634/21 OQ v Land Hessen, delivered on 16 March 2023, ECLI:EU:C:2023:220. paragragh 38; Judgment of the Court of Justice of 7 December 2023 OQ v Land Hessen, C-634/21, ECLI:EU:C:2023:957, paragraphs 44- 46. In paragraph 45, the Court, in particular, considered that "*The broad scope of the concept of 'decision' is confirmed by recital 71 of the GDPR, according to which a decision evaluating personal aspects relating to a person, to which that person should have the right not to be subject, 'may include a measure' which either produces 'legal effects concerning him or her', or, 'similarly significantly affects him or her*"'.

to an automated decision according to Article 22 GDPR, notably when they can have serious consequences for individuals.[103]

85. This could be the case, in particular, where the recommender system presents recommendations that cause effects that significantly affect data subjects, i.e. the 'decision' to present specific content to an individual may have an impact that is not necessarily legal but rather economic and social.[104] Particular attention should be paid to cases where 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, e.g. recommender systems for housing or job offers on an online platform. The DSA underlines the implications for data subjects related to recommender systems stating that "*recommender systems can have a significant impact on the ability of recipients to retrieve and interact with information online, including to facilitate the search of relevant information for recipients of the service and contribute to an improved user experience. They also play an important role in the amplification of certain messages, the viral dissemination of information and the stimulation of online behaviour*".[105]

86. Providers of online platforms act, according to the GDPR, as controllers in relation to personal data processed by recommender systems they decide to embed into their services. Along with the need to respect all other relevant GDPR provisions, providers shall, in particular, provide appropriate transparency obligations in relation to personal data processing in their recommender systems, in line with the requirements of Articles 12, 13 and 14 GDPR, including Articles 13(2)(f) and 14(2)(g) GDPR, if and when Article 22(1) GDPR applies.[106] In the same line, the EDPB welcomes that Article 27 DSA requires that providers of online platforms must be transparent with users in relation to the main parameters used in the recommender systems they embed into their services, and that they, where several options are available, shall make available a functionality that allows recipients of the service to, at any time, select and modify their preferred option of main parameters used in the recommender systems. In particular, providers must clarify in their terms of service, using an easy understandable form, "*why certain information is suggested*" or prioritised, why in a certain order and with a certain prominence of information displayed, 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, by granting them the

[103] Article 29 Data Protection Working Party Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, last revised and adopted on 6 February 2018, page 21, clarifies that "*For data processing to significantly affect someone the effects of the processing must be sufficiently great or important to be worthy of attention. In other words, the decision must have the potential to:*

- *significantly affect the circumstances, behaviour or choices of the individuals concerned;*
- *have a prolonged or permanent impact on the data subject; or*
- *at its most extreme, lead to the exclusion or discrimination of individuals*."

[104] Opinion of Advocate General Pikamäe in Case C-634/21 OQ v Land Hessen, delivered on 16 March 2023, ECLI:EU:C:2023:220. paragragh 38.

[105] See Recital 70 DSA.

[106] This involves, where processing is covered by Article 22(1) GDPR, telling "the data subject that they are engaging in this type of activity; provide meaningful information about the logic involved; and explain the significance and envisaged consequences of the processing". (...) "If the automated decision-making and profiling does not meet the Article 22(1) definition, it is nevertheless good practice to provide the above information. In any event the controller must provide sufficient information to the data subject to make the processing fair, and meet all the other information requirements of Articles 13 and 14". See Article 29 Data Protection Working Party Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, last revised and adopted on 6 February 2018 , page 25.

ability to modify options. Those options should be easily accessible from the online interface where the recommendations are presented.[107]

87. Article 38 DSA applies specifically to providers of VLOPs and of VLOSEs and applies in addition to Article 27 DSA. According to Article 38 DSA, such providers have to provide at least one option for each of their recommender systems which is not based on profiling as defined by GDPR.[108] The EDPB welcomes this provision and recalls that, in providing different options for recommender systems to users, providers of online platforms should respect the principle of data minimisation and the requirements of data protection by design and by default under Article 5(1)(c) and Article 25 GDPR. Therefore, providers of VLOPs and VLOSEs should present both options equally (on first use of the service) and should not nudge recipients of the service to select the option for a recommender system that is based on profiling.[109] Providers of VLOPs and VLOSEs may only use a recommender system based on profiling after the recipient of the service has chosen this option. In addition, while the non-profiling based option is active, the provider of the online platform cannot lawfully continue to collect and process personal data to profile the user, for the purposes of future recommendations, e.g. to be prepared in case the user chooses the profiling-based option or to provide more relevant recommendations because they would be based on a more detailed profiling. In addition, where a user uses both versions of a recommender systems, for example by switching several times in the same day, i.e. the version based on profiling and the version not based on profiling, then that user should not be profiled during the use of the version not based on profiling.

88. While Articles 27 and 38 DSA set out concrete safeguards for natural persons, users of online platforms and search engines, these safeguards involve further processing of personal data. As a consequence, the EDPB underlines that the collection and the processing of users' choices related to the modification of recommender systems parameters, should be processed by providers of online platforms and search engines for the sole purpose of complying with the DSA and stored only for the time necessary. Providers should not retain a history of previous choices either.

2.6 Protection of minors (Article 28)

89. One of the objectives of the DSA is the online protection of minors. In line with this objective, Article 28 DSA provides that "[p]roviders of online platforms accessible to minors shall put in place appropriate and proportionate measures to ensure a high level of privacy, safety, and security of minors, on their service". In addition, "[p]roviders of online platform shall not present advertisements on their interface based on profiling […][110] using personal data of the recipient of the service when they are aware with reasonable certainty that the recipient of the service is a minor". Article 28(3) DSA adds that, in the context of compliance with such obligations, there is no obligation for providers of online

[107] Article 27(3) DSA.
[108] According to Recital 9 DSA, "providers of very large online platforms and of very large online search engines should consistently ensure that recipients of their service enjoy alternative options which are not based on profiling, within the meaning of Regulation (EU) 2016/679, for the main parameters of their recommender systems. Such choices should be directly accessible from the online interface where the recommendations are presented."
[109] Cf. EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, version 2.0, Adopted on 20 October 2020, example 1 on page 19: the provider of the VLOP or VLOSE should not "*present the options in a way that nudges the data subject in the direction of allowing the controller to collect more personal data than if the options were presented in an equal and neutral way. This means that they cannot present the processing options in such a manner that makes it difficult for data subjects to abstain from sharing their data, or make it difficult for the data subjects to adjust their privacy settings and limit the processing*".
[110] As defined in Article 4(4) GDPR.

platforms "to process additional personal data in order to assess whether the recipient of the service is a minor".

90. In order to provide the high-level of privacy, safety and security for minors, as required pursuant to Article 28(1) DSA, providers of online platforms should understand the risks their services may pose to minors (e.g., exposure to harmful and/or illegal content, privacy risks, risks to health and wellbeing, and risks from advanced technology) so as to adapt the technical and organisational measures they take in response to these risks in the most appropriate and effective way. When measures taken to ensure a high level of privacy, safety, and security of minors (e.g., adoption of standards or participation in codes of conduct for protecting minors, age assurance, parental control or abuse signalling tools, etc.) involve the processing of personal data, controllers will need to assess the necessity and proportionality of the processing of personal data. There are other means than processing (additional) personal data through which the provider of an online platform may be aware that its service is used by minors, e.g., "when its terms and conditions permit minors to use the service, when its service is directed at or predominantly used by minors [by reason of certain features or content promoted on the service], or where the provider is otherwise aware that some of the recipients of its service are minors, for example because it already processes personal data of the recipients of its service revealing their age for other purposes"[111].

91. While there may be possibilities to ensure a high level of privacy, safety and security of minors, as laid down in Article 28(1) DSA, without processing of personal data, Article 28(1) DSA does not prohibit the processing of personal data as long as the processing adheres to the general requirements of the GDPR. Moreover, from the perspective of EU data protection law, providers of online platforms should ensure a high level of privacy, safety and security for all its users (not only minors), notably one that is appropriate to the risks of the processing. Such an approach is also relevant where a provider does not process (additional) personal data to determine with reasonable certainty whether a recipient of the service is a minor.

92. The GDPR requires a legal basis for the processing of personal data. Article 28(1) and (2) DSA envisages obligations that have to be respected by providers in very different situations and therefore, where personal data are to be processed to comply with such obligations, controllers have to ensure their lawful processing, taking into account the specificities of each case.[112] In this context, Articles 28(1) and (2) DSA can qualify as a legal basis for processing under Article 6(1)(c) GDPR to process personal data subject to the condition that the controller is able to demonstrate (on a case-by-case basis) that such processing (e.g., in the context of age assurance) is necessary and proportionate to achieve the goals established by Articles 28(1) and (2) DSA, taking into account the requirements of Article 6(3) GDPR. In any case, Article 28(3) DSA clarifies that providers of online platforms are not obliged to process (including collection and storage) additional personal data in order to assess whether the recipient of their service is a minor.[113] Processing that relies on Article 6(1)(c) GDPR must be (demonstrably) necessary and proportionate to the legitimate objective pursued, meaning that there must be no other

[111] Recital 71 DSA.

[112] Cf. European Commission, "Commission guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Article 28(4) of Regulation (EU) 2022/2065, C(2025) 4764 final, available at https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-protection-minors.

[113] Article 28(3) and Recital 71 DSA. This provision is also aligned with the spirit of the data minimisation principle under Article 5(1)(c) GDPR. This is especially important to consider when handling the result of the assessments carried out by the provider of the online platform, who should, for example, not store the age or age range of the recipient.

less intrusive means which, at the same time, would be as effective to pursue the objective.[114] As far as the processing of data falling under Article 9(1) GDPR is concerned, a controller will have to assess on a case-by-case basis whether it can rely on one of the derogations provided under Article 9(2) GDPR. However, processing of special categories of data, e.g. biometric data for the purpose of uniquely identifying a natural person, should be avoided, especially when children's data are expected to be processed.

93. 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.[115] Therefore, providers of online platforms should in particular avoid age assurance mechanisms that enable unambiguous online identification of their users (e.g., by asking them to submit proof of their identification via government-issued ID) on the basis of Article 28 DSA alone.

94. If an online platform provider concludes, after conducting an assessment, that age assurance is necessary for its platform, 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).[116] Additionally, providers of online platforms should not estimate or verify and permanently store the age or age range of the recipient of the service as a result of their age assurance process, but rather merely record whether the recipient of the service fulfils the condition(s) to use the service, thus implementing the principles of data minimisation and data protection by design and by default.[117]

95. If a provider operates an online platform that is designated as a VLOP, the obligations under Section 5 DSA also apply, including the obligations under Articles 34 and 35 DSA.[118] In that case, the provider must carry out an assessment of systemic risks stemming from its service and, if necessary, implement appropriate measures to mitigate such risks. According to Article 35(1)(j) DSA, possible risk mitigation measures for the protection of minors may include "targeted measures to protect the rights of the child, including age verification and parental control tools, tools aimed at helping minors signal abuse or obtain support". Read together, the requirements of Articles 28 and 35 DSA in conjunction with the GDPR mean that, e.g., age assurance should be carried out depending on the risk for minors and taking into account the necessary and proportionate processing of personal data, with particular consideration to the impacts of such measures on fundamental rights of the recipients of the service. Consequently, where the provider has concluded that there are only low risks affecting minors as recipients of the service and there are demonstrably no other means through which the provider of an online platform may become aware with reasonable certainty that a user is a minor,[119] it may therefore be

[114] Judgment of the Court of Justice of 9 November 2023 Gesamtverband Autoteile-Handel eV v Scania CV AB, C-319/22 ECLI:EU:C:2023:837, paragraphs 52 to 62.
[115] E.g. with privacy-preserving technologies, such as zero knowledge proofs, or any other technology given the state of the art. Cf. Recital 14 of the European Digital Identity Regulation (eIDAS 2.0) where 'age' is in the minimum list of attributes in Annex VI. In low-risk situations, it may be appropriate to provide the year of birth or to complete a form, although such measures may not be watertight in all cases. See EDPB Guidelines 05/2020 on consent under Regulation 2016/679, version 1.1, Adopted on 4 May 2020, paragraph 135.
[116] See also EDPB Statement 1/2025 on Age Assurance, Adopted on 11 February 2025, in particular section 2.2.
[117] Article 5(1)(c) and 25 GDPR.
[118] See also Section 2.7 of these guidelines.
[119] Cf. Paragraph 91.

sufficient to ask for confirmation that the user is above a relevant threshold and, in case of doubt, to carry out further checks[120] or to take measures that benefit all users, without making a distinction as to whether the service is used by a minor or not. When and which necessary and proportionate measures are required may not necessarily derive from the DSA or the GDPR[121], but also, for example, from other instruments of EU or Member State law[122]. In any case, the GDPR sets out requirements that appropriate and proportionate age assurance mechanisms should consider in relation to the processing of personal data.[123]

96. For further considerations on the processing of personal data in the context of age assurance, see the EDPB Statement on Age Assurance.[124]

2.7 Risk assessment and mitigation (Articles 34 and 35)

97. Articles 34 and 35 DSA oblige providers of VLOPs and of VLOSEs to manage systemic risks. The DSA does not define systemic risks. However, Article 34(1) DSA clarifies that the assessment of systemic risks should include a) the dissemination of illegal content, b) any actual or foreseeable negative effects for the exercise of fundamental rights, including Articles 7 and 8 of the Charter, i.e. the fundamental rights to privacy and data protection, c) any actual or foreseeable negative effects on civic discourse and electoral processes[125], and public security, and d) any actual or foreseeable negative effects in relation to gender-based violence, the protection of public health and minors and serious negative consequences to the person's physical and mental well-being.[126] Systemic risks, in the context of VLOPs and VLOSEs, have the potential to cause wider economic, societal and political harm that is not limited to individual users, but can also affect individual users.

98. Article 34(2) DSA provides a non-exhaustive list of factors that are assumed to influence the systemic risks, including the recommender system, the content moderation systems, the terms and conditions and their enforcement, advertisement, and data related practices of the provider.[127] Additionally, intentional manipulation of the service and dissemination of illegal content should be assessed. These factors are usually associated with the processing of personal data or are only made possible by it and must therefore meet the requirements of the GDPR. Particularly important in this context are the EDPB

[120] Cf. EDPB Guidelines 05/2020 on consent under Regulation 2016/679, version 1.1, Adopted on 4 May 2020, paragraph 135: "*If doubts arise, the controller should review their age verification mechanisms in a given case and consider whether alternative checks are required*".
[121] E.g. Article 8 and 24 GDPR.
[122] See e.g., Article 28b(3)(a) of Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities, PE/33/2018/REV/1, OJ L 303, 28.11.2018, p. 69–92.
[123] E.g. Article 25 GDPR.
[124] EDPB Statement 1/2025 on Age Assurance, Adopted on 11 February 2025.
[125] European Commission, "Commission publishes guidelines under the DSA for the mitigation of systemic risks online for elections", https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1707, 26 March 2024.
[126] See Recitals 80 to 83 DSA.
[127] This includes, according to Recital 79 DSA, the way in which the service is designed to benefit the often advertising-driven business models.

Guidelines on the Targeting of Social Media Users and the EDPB Guidelines on Deceptive Design Patterns.[128]

99. Part of the risk assessment is, according to Article 34(1)(b) DSA, the assessment of systemic risks for any actual or foreseeable negative effects for the exercise of fundamental rights, including among others Articles 1, 7, 8, 11, 21, 24 and 38 of the Charter.[129] Certain sources of such risks are further elaborated in Recital 81 DSA, e.g. in relation to the design of the algorithmic system, which should be adjusted, [130] where necessary after an assessment on a case-by-case basis, for example by taking measures to prevent or minimise biases that lead to the discrimination of persons in vulnerable situations, in particular where special categories of data according to Article 9 GDPR are processed.[131] Potential ways of tackling such possible risks include appropriate implementation of data protection by design and by default under Article 25 GDPR and the adoption of mitigating measures in Article 35(1)(d) DSA. In the case of a systemic risk affecting the fundamental right to the protection of personal data, that is additionally not limited to individual users, a data protection impact assessment (DPIA) pursuant to Article 35 GDPR will likely be mandatory.[132] In any case, it should be assessed whether the processing fulfils two or more of the criteria from the Article 29 Data Protection Working Party Guidelines on DPIA and, in some cases, a data controller can consider that a processing meeting only one of these criteria requires a DPIA.[133] In addition, it should be noted that the GDPR requires the processing of personal data in accordance with lawfulness, fairness and transparency and free from discrimination, in particular with Articles 5, 22, 24 and 25 as well as Recitals 71 and 75 GDPR.[134]

100. For a possible mitigation of systemic risks, the DSA provides in Article 35 a list of exemplary measures that may be applied by the providers of VLOPs and VLOSEs. In any event, Article 35(1) DSA requires measures to be reasonable, proportionate and effective in mitigating the specific systemic risks identified. The remainder of this section describes measures that are directly related to the GDPR, without implying that the other measures do not have to be implemented in compliance with the GDPR.

101. As an example, Article 35(1)(f) DSA lists internal processes, resources, testing, documentation and supervision which can be, inter alia, helpful to demonstrate effectiveness. In addition, Article 35(1)(f) DSA concerns the possibility to reinforce these measures in particular as regards detection of systemic

---

[128] EDPB Guidelines 8/2020 on the targeting of social media users, version 2.0, Adopted on 13 April 2021; EDPB Guidelines 3/2022 on Deceptive design patterns in social media platform interfaces: how to recognise and avoid them, version 2.0, Adopted on 14 February 2023.

[129] Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012, p. 391–407.
Article 8 of the Charter contains the fundamental right for the protection of personal data.

[130] See Article 35(1) DSA.

[131] See Recital 94 DSA.

[132] Criteria for a sufficiently comprehensive DPIA can be found in Article 29 Data Protection Working Party Guidelines on Data Protection Impact Assessment (DPIA) and determining the criteria whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP 248 rev.01, 4 October 2017.

[133] Ibid. p. 9 ff. The criteria are 'evaluation or scoring', 'automated-decision making with legal or similar significant effect' 'systematic monitoring', 'sensitive data or data of a highly personal nature', 'data processed on a large scale', 'matching or combining datasets', 'data concerning vulnerable data subjects', 'innovative use or applying new technological or organisational solutions' and when the processing itself 'prevents data subjects from exercising a right or using a service or a contract'.

[134] Cf. EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, version 2.0, Adopted on 20. October 2020, in particular paragraphs 69 f.; cf. Judgment of the Court of Justice of 7 December 2023, OQ v Land Hessen, C-634/21, ECLI:EU:C:2023:957,, in particular paragraphs 59 and 66.

risks. This is also "at the heart of the concept of data protection by design"[135] and the EDPB Guidelines on Article 25 GDPR complement this requirement with, for example, key performance indicators and with the rationale for the assessment of the effectiveness. It should be noted that such measures are also necessary in the operation of an application and are not limited only to the development. Such measures include, according to Article 32(1)(d) GDPR, a process to regularly test, assess and evaluate the effectiveness of the technical and organisational measures to ensure the security of the processing and, according to Article 33 GDPR and Recital 87 GDPR, appropriate measures to determine whether there have been relevant deviations from the compliant operation leading to a breach.

102. Article 35(1)(a) DSA elaborates on the mitigating measure of "adapting the design, features or functioning of their services, including their online interfaces", which overlaps with the obligation of a controller to design a system for processing personal data in accordance with the requirements of data protection by design and by default under Article 25 GDPR. With regard to systemic risks that can stem, for example, from (automated) tools for detecting illegal content or illegal activities,[136] recommender systems and advertising systems, adhering to GDPR principles and safeguards, including data minimisation as well as the use of technical and organisational measures, such as pseudonymisation, can enable providers of very large online platforms and very large online search engines, to effectively comply with the requirements of the DSA, including Article 35 DSA.[137] It should be noted here that Article 35 DSA requires providers to take into account the impact of measures they take to mitigate systemic risks on fundamental rights in general. Article 5 and 25 GDPR oblige controllers to process personal data only to the extent necessary for each specific purpose, taking into account the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility.

103. Article 35(1)(d) DSA lists as a possible measure to test and adapt the algorithmic systems, including the recommender systems, and Article 35(1)(e) DSA mentions that providers can adapt their advertising systems to comply with the requirements of the DSA. Recommender systems and advertising may involve the processing of personal data and the GDPR applies, in particular in relation to the collection of personal data and use practices (cf. Recital 84 DSA). A comprehensive analysis of this issue can be found in the EDPB Guidelines on Targeting of Social Media Users, which identifies several risks, including the data subject's ability to control his or her personal data, discrimination and exclusion, manipulation of data subjects, and 'may involve unanticipated or undesired uses of personal data, which raise questions not only concerning data protection law, but also in relation to other fundamental rights and freedoms'.[138]

104. The measures to inform users referred to in Article 35(1)(i) DSA are consistent with Articles 13 and 14 GDPR insofar as personal data are processed. The provider should ensure that the information necessary to ensure fair and transparent processing is provided to data subjects.[139]

---

[135] EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, version 2.0, Adopted on 20 October 2020, paragraphs 13 ff, in particular paragraph 16.
[136] Including notice and action mechanisms under Article 16 DSA and content moderation processes under Article 35(1)(c) DSA.
[137] Article 25(1) GDPR.
[138] EDPB Guidelines 8/2020 on the targeting of social media users, version 2.0, Adopted on 13 April 2021, paragraph 4.
[139] Article 29 Data Protection Working Party Guidelines on transparency under Regulation 2016/679, WP 260 rev.01, 11. April 2018.

105. Recital 81 DSA clarifies that "[w]hen assessing risks to the rights of the child, providers of very large online platforms and of very large online search engines should consider for example how easy it is for minors to understand the design and functioning of the service, as well as how minors can be exposed through their service to content that may impair minors' health, physical, mental and moral development. Such risks may arise, for example, in relation to the design of online interfaces which intentionally or unintentionally exploit the weaknesses and inexperience of minors or which may cause addictive behaviour." Furthermore, Article 35(1)(j) DSA mentions that providers can take "targeted measures to protect the rights of the child, including age verification and parental control […]". When a provider considers that age verification would a be a reasonable, proportionate, and effective mitigation measures, tailored to the specific systemic systemic risk(s) identified, age verification methods must, in particular, take into account the requirements of Articles 5 to 8 and 25 GDPR, and, if applicable, Article 22 GDPR.[140] For further considerations, see the EDPB Statement on Age Assurance.[141]

106. The list of possible measures in Articles 35(1) DSA is very helpful for providers of VLOPs and VLOSEs, as well as for DSA supervisory authorities and data protection supervisory authorities, and it should be considered in a risk assessment according to Article 35 GDPR. The EBDS, in cooperation with the Commission will publish reports on best practices in the mitigation of systemic risks (Article 35(2) DSA), and the Commission can issue application guidelines concerning risk mitigation measures as provided for in Article 35(3) DSA.

107. In conclusion, providers of VLOPs and VLOSEs are obliged under Article 34 DSA to carry out a risk assessment for systemic risks including, inter alia, risks to the protection of personal data according to Article 8 of the Charter which the GDPR reflects in secondary law. If there are systemic risks, a DPIA according to Article 35 GDPR is likely to be mandatory.

2.8 Codes of conduct, including for online advertising (Articles 45, 46 and 47), and their relationship with codes of conduct under Article 40 GDPR

108. Article 45 DSA requires the Commission and the Board to encourage and facilitate the drawing up of voluntary codes of conduct at Union level to contribute to the proper application of the DSA "taking into account in particular the specific challenges of tackling different types of illegal content and systemic risks, in accordance with Union law in particular on competition and the protection of personal data".

109. Article 45(2) DSA enables the Commission to invite "relevant stakeholders" to participate in the drawing up of codes of conduct, including by setting out commitments to take specific risk mitigation measures, as well as a regular reporting framework on any measures taken and their outcomes. Given the interplay between the risk assessment and mitigation measures under the DSA and GDPR, it is important to ensure appropriate involvement of data protection authorities, as well as to clarify the relationship between Codes of conduct under the DSA and codes of conduct under the GDPR. This consideration applies even more so in the context of the development of codes of conduct for online advertising under Article 46 DSA.

110. In order to be able to monitor the achievement of the commitments, the codes of conduct should contain measurable key performance indicators.[142] Such key performance indicators can be used to continuously measure the effectiveness of the measures and are also proposed in the EDPB Guidelines

[140] See also Section 2.6 of these guidelines, paragraph 96.
[141] EDPB Statement 1/2025 on Age Assurance, Adopted on 11 February 2025.
[142] Article 45(3) DSA.

4/2019 on Article 25 Data Protection by Design and by Default (cf. section 4.6, paragraph 97). Ideally, the DSA and GDPR codes of conduct should be complementary at this point.

111. In Article 46 DSA, providers in the advertising value chain are encouraged to contribute to further transparency beyond the requirements of Article 26 and 39 DSA. This could include, for example, the transparency requirements of Chapter 3 GDPR.

112. This objective is further elaborated in Article 47 DSA, which addresses the accessibility of online services for people with disabilities and includes the appropriate design of the service and making information easy to find, easy to understand, and accessible to persons with disabilities (cf. Recital 58 GDPR). A comprehensive discussion of this topic can also be found in the EDPB Guidelines on transparency under Regulation 2016/679.[143]

2.9 Governance and Enforcement

113. As shown above, several obligations imposed on intermediary service providers (including VLOPs and VLOSEs) under the DSA include provisions that affect the processing of personal data by intermediary service providers and specifically refer to definitions and concepts under the GDPR. The EDPB recalls that according to Article 8(3) of the Charter, compliance with the GDPR shall be subject to control by an independent authority.[144]

2.9.1 Cooperation between competent authorities and duty of sincere cooperation with DPAs

114. The DSA provides that Member States shall designate one or more competent authorities to supervise and enforce this Regulation.[145] These national competent authorities could be already existing ones, and the DSA makes an explicit reference to the possibility for Member States to designate electronic communications' regulators, media regulators or consumer protection authorities.[146] In case a Member State has provided for multiple competent authorities with specific tasks related to the DSA, they shall cooperate closely and effectively, and one of them shall be designated by each Member State as the DSC to ensure the coordination at national level.[147] The EDPB acknowledges that while several provisions of the DSA are relevant from a data protection perspective, Member States may designate national competent authorities other than data protection supervisory authorities to supervise and enforce these provisions.

115. The DSA provides that DSCs shall cooperate with each other, other national competent authorities, the European Board for Digital Services and the European Commission, without prejudice to the possibility for Member States to provide for cooperation mechanisms and regular exchanges of views between the DSCs and other national authorities where relevant for the performance of their respective tasks.[148] Therefore, in the scenario where a Member State chooses not to designate the data protection supervisory authority as one of the competent authorities to supervise and enforce provisions

[143] Article 29 Working Party Guidelines on transparency under Regulation 2016/679 (WP260 rev.01), as last Revised and Adopted on 11 April 2018.
[144] Article 52 GDPR establishes rules to ensure the independence of the supervisory authorities designated in each EU Member State, which build on Article 8(3) of the Charter and on case law of the CJEU on the requirement of independence under the predecessor of the GDPR, Article 28(1) of Directive 95/46/EC.
[145] Article 49(1) DSA.
[146] Recital 109 DSA.
[147] Article 49(2) DSA.
[148] Article 49(2) DSA.

related to the protection of personal data under the DSA, the DSA does not prevent Member States from establishing cooperation mechanisms and regular exchanges under their national framework between the DSC and data protection supervisory authorities. This could be necessary, for example, in cases where a data protection supervisory authority may issue an order to act against one or more specific items of illegal content on the basis of the data protection law (e.g., an order to delete personal data following a request of a data subject under Article 17 GDPR that was not honored by the controller) and Article 9 DSA will need to be applied. The EDPB encourages Member States to take these situations into account and identify effective cooperation mechanisms that allow that Member State to streamline the work of the different actors that may need to intervene in the contexts covered by the DSA.[149]

116. The DSA provides that the European Commission shall have exclusive powers of supervision and enforcement of the additional obligations resulting from Section 5 of Chapter III of the DSA imposed on providers of VLOPs and of VLOSEs.[150] The powers of supervision and enforcement against VLOPs and VLOSEs of obligations other than the ones resulting from Section 5 of Chapter III of the DSA are shared between the European Commission and the national competent authorities.[151] National competent authorities may only initiate proceedings against VLOPs and VLOSEs where the European Commission has not yet done so for the same infringement[152] in the interest of efficiency, to avoid duplication and to ensure compliance with the principle of ne bis in idem,[153] and both are required to enforce the DSA in close cooperation.[154]

117. While the DSA provides rules of tasks distribution between the European Commission and DSCs to avoid duplication, inconsistencies and risks related to the principle of *ne bis in idem* under the DSA, the DSA does not provide for an explicit duty of consultation and cooperation with data protection supervisory authorities for ensuring regulatory consistency with the GDPR, notably for the handling of concrete enforcement cases. However, according to Article 64(3) DSA, "the Commission may ask […] other Union bodies, offices and agencies with relevant expertise to support the assessment of systemic and emerging issues across the Union under this Regulation*".* Moreover, Recital 143 foresees the possibility of the European Commission appointing independent external experts or auditors from data protection authorities to assist in monitoring the effective implementation of and compliance with the obligations laid down in the DSA. The EDPB welcomes these provisions which have the potential to contribute to the dialogue between the Commission and data protection supervisory authorities, either because they are competent authorities under the DSA or because they have relevant expertise, for the consistent application of the DSA and the GDPR.

118. Neither the GDPR nor the DSA provide for specific rules on cooperation between competent authorities under the DSA and data protection supervisory authorities. However, in light of Article 8(3) of the Charter and the principle of sincere cooperation under Article 4(3) TEU as interpreted by the CJEU,[155] when authorities with competences for the enforcement of the DSA (including the European Commission) are called upon, in the exercise of their powers, to examine whether an intermediary services

[149] See EDPB Position paper on Interplay between data protection and competition law, Adopted on 16 January 2025, for examples of cooperation mechanisms, and notably Section 4.3 on "Ways to improve cooperation".
[150] Article 56(2) DSA.
[151] Articles 56(3) DSA.
[152] Article 56(4) DSA.
[153] Recital 125 DSA.
[154] Article 56(5) DSA.
[155] Judgment of the Court of Justice of 4 July 2023 Meta Platforms and others, C-252/21, ECLI:EU:C:2023:537.

provider's conduct is consistent with the provisions of the GDPR[156], they should consult and cooperate sincerely with the national data protection supervisory authorities concerned or with the lead data protection supervisory authority. Conversely, when data protection supervisory authorities are called upon, in the exercise of their powers, to examine whether a controller's or processor's conduct is consistent with the provisions of the DSA, they should consult and cooperate sincerely with the authorities with competences for the enforcement of the DSA (including the European Commission). The consultation of a competent authority under a different framework should take place, inter alia, when the consulted authority has issued a decision concerning the conduct (or similar conduct) of the intermediary service provider that is under assessment by the consulting authority.

119. Such cooperation would not only benefit data subjects, but also intermediary service providers by improving legal certainty of how the DSA on the one hand and the GDPR, on the other, are applied. It would also contribute to avoid duplication of efforts, and legal risks related to regulatory inconsistencies with regard to the supervision of intermediary services providers. This is also important to ensure that a potential duplication of procedings and penalities by authorities with competences for the enforcement of the DSA (including the European Commission) and data protection supervisory authorities does not lead to an infringement of the non bis in idem principle.[157]

120. Where a data protection supervisory authority is consulted by a competent authority enforcing the DSA, it should respond within a reasonable period of time by providing the latter with the information in its possession capable of dispelling that authority's doubts about the application of the GDPR.[158] Alternatively, the consulted data protection supervisory authority should, where appropriate, inform the authority with competences for the enforcement of the DSA if it intends to initiate the cooperation procedure with the other supervisory authorities concerned or with the lead supervisory authority, in accordance with Article 60 et seq. of the GDPR,[159] in order to reach a decision seeking to establish whether or not the conduct in question is consistent with the GDPR.[160] The consulting authority may continue its investigation if it does not receive a reply within a reasonable time from the consulted supervisory authority, or where the latter does not object to such an investigation being continued without having to wait for a decision on their part.[161]

---

[156] This is not the same as enforcing data protection law as such, which is the exclusive competence of data protection supervisory authorities. See Judgement of the Court of Justice of 4 July 2023 Meta Platforms and others,C-252/21, ECLI:EU:C:2023:537, paragraphs 44 and 45.

[157] In particular the CJEU stated that in analyzing whether a duplication of proceedings and penalties respects the essence of the *ne bis in idem* principle laid down in Article 50 of the Charter, "*it is necessary to assess whether there are clear and precise rules making it possible to predict which acts or omissions are liable to be subject to a duplication of proceedings and penalties,* ***and also to predict that there will be coordination between the different authorities, whether the two sets of proceedings have been conducted in a manner that is sufficiently coordinated*** *and within a proximate timeframe*". See Judgment of the Court of Justice of 22 March 2022 bpost SA v Autorité belge de la concurrence, C-117/20, ECLI:EU:C:2022:202, paragraphs 43 to 58.

[158] Judgment of the Court of Justice of 4 July 2023 Meta Platforms and others, C-252/21, ECLI:EU:C:2023:537, paragraphs 57 and 58.

[159] The cooperation and consistency mechanism provided for by Chapter VII of the GDPR do not apply to the enforcement of the provisions concerning the protection of personal data contained in the DSA as such. However, the cooperation and consistency mechanism remains fully applicable insofar as a processing is subject to the general provisions of the GDPR.

[160] Judgment of the Court of Justice of 4 July 2023 Meta Platforms and others, C-252/21, ECLI:EU:C:2023:537, paragraph 58.

[161] Judgment of the Court of Justice of 4 July 2023 Meta Platforms and others, C-252/21, ECLI:EU:C:2023:537, paragraph 59.

2.9.2 European Board for Digital Services

121. The European Board for Digital Services ('EBDS') established for advising on the supervision of providers of intermediary services under the DSA is chaired by the European Commission and composed of DSCs.[162] Other national authorities that have been designated as competent authorities under the DSA by their Member State (including, where applicable, data protection supervisory authorities) may participate in the Board alongside the DSC where provided for by national law. Other national authorities may be invited "*where the issues discussed are of relevance for them*"[163].

122. Moreover, "*the Board […] may cooperate with other Union bodies"*[164] with responsibilities in fields such as data protection.[165] The EDPB considers that cooperation between the EBDS and the EDPB would be important to ensure cross-regulatory consistency in the application of the DSA and the GDPR. Indeed, the tasks of the EBDS include supporting authorities with competences for the enforcement of the DSA in the analysis of reports and results of audits of VLOPs or of VLOSEs (such as risk assessments that analyse negative effects of digital services on the fundamental right to the protection of personal data)[166], supporting and promoting the development and implementation of European standards, guidelines, reports, templates and code of conducts in cooperation with relevant stakeholders as provided for in the DSA. Further, it shall support the identification of emerging issues, with regard to matters covered by the DSA.[167]

[162] Article 61 and 62 DSA.
[163] Article 62(1) DSA.
[164] Article 62(5) DSA.
[165] Recital 134 DSA.
[166] Article 34(1)(b) DSA.
[167] Article 63(1)(e) DSA.