Feedback to the European Data Protection Board's Guidelines 3/2025 on the interplay between the DSA and the GDPR (Version 1.1)

Dr. Cristiana Santos, Utrecht University, The Netherlands, c.teixeirasantos@uu.nl
Dr. Nataliia Bielova, Inria, France, nataliia.bielova@inria.fr
Dr. Johanna Gunawan, Maastricht University, The Netherlands, johanna.gunawan@maastrichtuniversity.nl
Dr. Brennan Schaffner, Georgetown University, USA, brennan.schaffner@georgetown.edu
Prof. Dr. Simone van der Hof, Leiden University, The Netherlands, s.van.der.hof@law.leidenuniv.nl
Dr. Arianna Rossi, Sant'Ana School of Advanced Studies, Italy, arianna.rossi@santannapisa.it
Marie-Therese Sekwenz, Delft University of Technology, The Netherlands, M.T.Sekwenz@tudelft.nl

Prof. Cristiana Santos is an Assistant Professor in *Data Protection Law* at Utrecht University (The Netherlands) and holds an International Chair position at Inria (France). She has been serving as an expert of the Data Protection Unit of the Council of Europe; an expert of the Digital Persuasion or Manipulation Expert Group in The Netherlands; she consults the EU Commission, OECD, Global Privacy Enforcement Network (GPEN), other policy-makers and civil society organizations. Prof. Santos has won multiple awards in Data Protection, including the Stefano Rodotà Data Protection Award of the Council of Europe, the European Cyber Women Day Winner, and the CNIL–Inria Privacy Award.

Dr. Nataliia Bielova is a Research Director in *Computer Science* at Inria (French Institute for Research in Computer Science and Automation). She is a privacy expert with a multidisciplinary background in *computer science and regulation*, investigating privacy and data protection on the Web. Dr. Bielova was a Senior Privacy Fellow at the French Data Protection Authority (CNIL) and an External Expert for the EU Commission for its implementation of the EU Digital Services Act (DSA). She received a Young Researcher Award from the French National Research Agency (ANR), the Rising Star award by Women at Privacy in 2023, the CNIL–Inria Privacy Award in 2025 and the Lovelace-Babbage Award from the French Science Academy and the French Computer Society in 2025.

Prof. Johanna Gunawan is an interdisciplinary Assistant Professor in *Computer Science and Law* at Maastricht University (The Netherlands). Her background spans cybersecurity and privacy, human-computer interaction, and policy, with her research focusing on digital consumer protection in the EU and the US. She has written extensively on dark patterns in multiple modalities and types of technologies, ranging from ubiquitous mobile and IoT interfaces to cutting-edge technologies like social robotics. Her work has been cited by the US FTC, as well as other regulators (UK CMA) and policy organisations (OECD).

Dr. Brennan Schaffner is a postdoctoral Fritz Fellow at Georgetown University (Washington, DC). He has published work on dark patterns related to social media and streaming video-on-demand platforms in leading human-computer interaction conferences. He worked directly with the FTC and their expert witness in recent litigation with Amazon involving dark patterns. Seated at the intersection of human-computer interaction and policy research, he also studies content moderation policies and tracks tech litigation in the United States.

Prof. Simone van der Hof is a full professor of law and digital technologies at the Center for Law and Digital Technologies at Leiden University. She has an extensive academic track record in children's rights and digital technologies, focusing on data protection, commercial exploitation, and behavioral design in video games. She was one of the authors of the Children's Rights Code.[1] She has co-developed a model for a Children's Rights Impact Assessment,[2] an Age Assurance Self-Assessment tool,[3] and was involved in developing a prototype for identifying manipulative design in video games.[4] One of her recent projects, which the European Commission commissioned, was on a Typology and Requirements for Age Assurance.[5] She holds various ancillary positions in age classification, online transgressive behavior, media literacy, and digital well-being.

Dr. Arianna Rossi is a research affiliate of the LIDER Lab at Sant'Anna School of Advanced Studies (Pisa, Italy) and is an expert in online manipulation, usable privacy, and legal design. She carries out empirical and theoretical research with a clear interdisciplinary slant, at the intersection of data law, human-centered design and computer science. She has been an invited speaker at international conferences and routinely gives about law, design and technology to academic students and practitioners.

Marie-Therese Sekwenz is a PhD candidate at TU Delft's Faculty of Technology, Policy and Management, where she serves as Deputy Director of the AI Futures Lab on Rights and Justice. An expert on the DSA and European platform regulation, her research examines the evolving landscape of content moderation, algorithmic governance, and regulatory compliance in digital environments, including deepened research on reporting mechanisms and legal design requirements of the NetzDG and the DSA. In addition to her academic work, she is active as a journalist for the Austrian Broadcasting Corporation (ORF), producing features for programs such as 'Diagonal' and 'Radiokolleg'. She previously worked on research projects at the Leibniz Institute for Media Research – Hans-Bredow-Institute (HBI) and the Vienna University of Economics and Business.

Hereunder is our feedback to the EDPB Guidelines 3/2025 on the interplay between the DSA and the GDPR[6] with regard to:

1. **notice and action mechanisms** (paragraphs 25-32),

[1] Code for Children's Rights, https://codevoorkinderrechten.waag.org/wp-content/uploads/2022/02/Code-voor-Kinderrechten-EN.pdf

[2] Hof S. van der, Challis L., Wanroij E. van & Schermer B.W. (2024), Child rights impact assessment: impact and legal analysis for the development of the CRIA. The Hague: Ministry for Internal Affairs and Kingdom Relations, http://hdl.handle.net/1887/4209969

[3] Shaffique M.R. & Hof S. van der (2024), Self-assessment tool on age assurance: Manual. Luxemburg: European Commission, http://hdl.handle.net/1887/4177486; Shaffique M.R. & Hof S. van der (2024), Self-assessment tool on age assurance: questionnaire. Luxemburg: European Commission, http://hdl.handle.net/1887/4177488

[4] van Rooij, A. J., Birk, M., & van der Hof, S. (2025). Game-check: Development, application and visualization of a classification system for behavioral design in games. Trimbos institute, Eindhoven University of Technology & Leiden University. https://www.trimbos.nl/wp-content/uploads/2025/10/Game-check-Development-application-and-visualization-of-a-classification-system-for-behavioral-design.pdf

[5] Shaffique M.R. & Hof S. van der (2024), Mapping age assurance typologies and requirements. Luxemburg: European Commission-Publications Office of the European Union, https://op.europa.eu/en/publication-detail/-/publication/215f6c72-fe04-11ee-a251-01aa75ed71a1/language-en

[6] https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2025/guidelines-32025-interplay-between-dsa-and-gdpr_en

2. **regulation of dark patterns** (paragraphs 43, 44, 45)
3. **addictive behavior** (paragraphs 46, 47) and
4. **minors** (paragraphs 90-95).

Hereunder is our feedback to the EDPB Guidelines 3/2025 on the interplay between the DSA and the GDPR.[7] We present general comments and comments per paragraph. Our comments are presented after a quotation from the proposed text in a box. The highlights in **bold** were added by the authors.

General comment on "deceptive design"

We express a general concern on the usage of the term "**deceptive design**" by the EDPB. The concept of "deception" has been extensively defined in the literature. Deception is a very narrow type of influence on the user, "*it covers any practice that creates in the user a perception that does not correspond to reality*"[8]. It "*induces false beliefs* that does not correspond to reality*, either through affirmative misstatements, misleading statements, or omissions*"[9]. In other words, deception is based on false information or influencing someone to hold false beliefs. We recommend the EDPB not to use the concept "deceptive design" as it limits the types of influences on the user's autonomy that are provided in the Article 25(1) of the DSA. We suggest considering the use of the term "dark patterns". Even though it has been recently criticised, there is no other term currently in use that describes the broad remit of dark patterns practices that include deceptive, manipulative, and coercive patterns that limit user agency and are often hidden to the user.

We want to draw the EDPB's attention to the fact that **dark patterns also operate beyond the traditional "user interfaces"**, including examples like deceptive *Countdown Timer* or *Limited Time Message* that is implemented with a JavaScript code on websites.

General comment on minors

Under the GDPR, children should enjoy a high level of data protection, as recognized in Recital 38 and various provisions, explicitly or implicitly. The specific level of protection for children's personal data has been further elaborated in WP29 and other EDPB guidelines. It has also been part of academic discourse since the adoption of the GDPR. Unfortunately, **EDPB guidelines on processing children's personal data are not ready yet. Article 28 DSA requires online platforms to provide a high level of privacy, safety, and security.** Adequate protection of children's personal data, in line with Recital 38, potentially benefits all three areas. The way

[7] https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2025/guidelines-32025-interplay-between-dsa-and-gdpr_en

[8] See pp.6-7 of "Understanding the scope of Article 25 of the DSA in regulating dark patterns." Cristiana Santos, Sanju Ahuja, Nataliia Bielova, and Christine Utz. Dark patterns and deceptive design patterns: Conceptualising and systematising a key contemporary phenomenon. R. Gellert, C. Santos, & H. Schraffenberger (Eds.), Edward Elgar. (2025, forthcoming). Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4899559

[9] See p. 6 of Arunesh Mathur, Jonathan Mayer, and Mihir Kshirsagar, What Makes a Dark Pattern... Dark?: Design Attributes, Normative Considerations, and Measurement Methods in: Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI '21), https://doi.org/10.1145/3411764.3445610

the draft EDPB guidelines on the interplay between DSA and GDPR guide a high level of privacy and data protection can be substantiated considerably.

Under the data protection principles in Article 5 GDPR, online platforms need to consider the processing of children's personal data specifically. **Fairness** concerns power imbalances between the data subject and controller and the user's expectations relating to data processing, and both raise particular considerations for children. The same is true for the principles of lawfulness, transparency, purpose limitation, and data minimization.[10] A high level of privacy under Article 28 (1) DSA builds on the high level of data protection for children as provided for in the GDPR; hence, a translation of data protection principles (as well as related other GDPR provisions) to the relationship between children and online platforms in light of providing a high level of privacy, safety and security is necessary. Still, **this is largely missing in the draft version.** In this respect, it is particularly relevant to focus on how **privacy by design and default** can protect children as part of the age-appropriate design of digital services.[11] Article 28 Guidelines from the European Commission[12] provide essential guidance on age-appropriate design that should be reflected in the EDPB Guidelines to the extent that they address providing children with a high level of privacy and data protection. Article 28 (3) is particularly relevant to processing personal data, as acknowledged in the EDPB Guidelines. However, behavioral advertising is only one form of commercial profiling of children that the GDPR and the DSA cover. In 2018, the Council of Europe already determined in its recommendations that the profiling of children should be prohibited unless it is in their best interests.[13] In 2021, the UN Committee on the Rights of the Child in its General Comment 25 stated that commercial profiling of children should be prohibited by law.[14] This explanation is also reflected in the emerging interpretation of Article 6(1)(a) (children cannot consent to profiling because of a lack of understanding) and Article 22 of the GDPR (no exceptions to the prohibition of automated profiling for children unless in their best interest).[15] I**t is essential that the EDPB Guidelines clearly set out the red lines for commercial profiling to the extent that it is not in the child's best interest, given that it can impact the privacy and safety of children and be a systemic risk under Article 34 DSA.** Also, in this case, alignment with the Article 28 Guidelines is required because there is an interplay between, e.g., recommendation systems and commercial practices addressed there. Moreover, various paragraphs address

[10] See for further elaboration and references, van der Hof, S., Lievens, E., & Milkaite, I. (2022). The GDPR and Children's Personal Data. In Oxford Encyclopia of EU Law. Oxford University Press.

[11] See also van der Hof, S., & Lievens, E. (2018). The importance of privacy by design and data protection impact assessments in strengthening protection of children's personal data under the GDPR. Communications Law, 23(1), 33-43.

[12] 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 (No. C(2025) 4764 final). (2025). European Commission. https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-protection-minors

[13] Council of Europe. (2018, september). Recommendation CM/Rec(2018)7 of the Committee of Ministers, Guidelines to respect, protect and fulfil the rights of the child in the digital environment. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016808b79f7

[14] Committee on the Rights of the Child. (2021, maart 2). General comment No. 25 (2021) on children's rights in relation to the digital environment. https://digitallibrary.un.org/record/3906061

[15] See for an extensive legal analysis of commercial profiling of children, Leijten, E., & van der Hof, S. (2025). Dissecting the commercial profiling of children: A proposed taxonomy and assessment of the GDPR, UCPD, DSA and AI Act in light of the precautionary principle. Computer Law & Security Review, 57, 106143. https://doi.org/10.1016/j.clsr.2025.106143

the interplay between the GDPR and age assurance under Article 28, which does not contribute to the guidelines' readability.

Comments paragraph by paragraph

Our remaining comments are presented after a quotation from the proposed text in a box. The highlights in bold were added by the authors.

> 2 SPECIFIC ISSUES
>
> 2.1 Voluntary own-initiative investigations and legal compliance in relation to illegal content (Article 7)
>
> 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').

Definition on illegal content

In the definition of illegal content for the DSA and the understanding of the intersection of the DSA and the GDPR, **having an actionable definition of what can be seen as illegal is necessary**. Recital 12 DSA already links back to the heterogeneity of the member state's definition of illegal content. As illustrated in Wagner et al., the member states chose different sets of norms that might classify as illegal – ending up in several sources of norms from criminal law, to trademark law or copyright law or privacy related civil law rules.[16] These may differentiate in member states and are especially relevant to make actionable for regulators, public authorities and platforms resulting in differences in reporting mechanism design. Also influencing users and trusted flaggers tasks to understand how to interact with reporting mechanisms in border crossing cases. We recommend the EDPB to provide an actionable definition of illegal content.

> 2.2.1 Processing activities involved by the notice and action mechanisms (Articles 16 DSA)
>
> Paragraphs 25-37

[16] Ben Wagner and others, 'Mapping Interpretations of the Law in Online Content Moderation in Germany' (2024) 55 Computer Law & Security Review 106054.

Design solutions within 'Notice and Action' mechanisms can conflict with the minimization principles

Notice and action mechanisms and internal complaint-handling systems may also entail the processing of personal data, notably since service providers must implement mechanisms for reporting illegal content, allowing individuals or entities to notify, by electronic means, the presence of specific items of information that they consider to be illegal content, which constitutes a complex design problem.[17] While there is an exception allowing the provision of personal data in cases involving CSAM, it is problematic that no similar exception exists for other high-risk areas such as terrorist content. For example, requiring whistle blowers to provide identifying information like their name or email address could expose them to significant harm. As a result, users who would otherwise report illegal content may hesitate to do so out of concern for their privacy, choosing instead to report such material only under the platform's general terms of service to protect their anonymity. This might result in skewed reporting in transparency reports, the Statement of Reason database and user harm.[18]

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"

These mechanisms also are used by Trusted Flaggers.[19] However**, current design solutions of reporting mechanisms do not allow the differentiation of different types of users,** like 'regular' users, trusted flagger programs (certified by the platform), or trusted flaggers (certified by the Digital Service Coordinators). As a result, all users are required to provide the same information. This lack of differentiation overlooks the fact that **expert users, such as Trusted Flaggers, may have a better understanding of the implications of personal data sharing and the potential consequences of providing personal data.**

Additionally, th**e current design of reporting mechanisms and the information provided to lay users do not clarify whether submitting a notification could result in data being shared with public authorities or lead to potential legal consequences for the user** (for example, their report being used as evidence in a case). It is also not transparent for which flags or legal norm notice categories such implications may arise—for instance, in which cases a user might be considered a witness, or their report might serve as evidence in court or other public authority proceedings.[20]

[17] Marie-Therese Sekwenz, Daria Simons and Alina Wundsam, 'Prompt Template for a Fictitious LLM Agent in a Content-Flagging Experiment' (arXiv, 29 July 2025) <http://arxiv.org/abs/2507.21842> accessed 19 August 2025.

[18] Marie-Therese Sekwenz, Ben Wagner and Hans De Bruijn, 'From Reports to Reality: Testing Consistency in Instagram's Digital Services Act Compliance Data' (arXiv, 2 July 2025) <http://arxiv.org/abs/2507.01787> accessed 9 July 2025; Ben Wagner and others, 'Regulating Transparency? Facebook, Twitter and the German Network Enforcement Act', *Proceedings of the* 2020 Conference on Fairness, Accountability, and Transparency (Association for Computing Machinery 2020) <https://dl.acm.org/doi/10.1145/3351095.3372856> accessed 12 August 2025.

[19] Marie-Therese Sekwenz and Rita Gsenger, 'The Digital Services Act: Online Risks, Transparency and Data Access', *Digital Decade – How the EU Shapes Digitalisation Research*.

[20] Marie-Therese Sekwenz, Ben Wagner and Simon Parkin, '"It Is Unfair, and It Would Be Unwise to Expect the User to Know the Law!" – Evaluating Reporting Mechanisms under the Digital Services Act', *Proceedings of the*

28. **With regard to personal data of the 'notifier'50, with a view to facilitating the submission of sufficiently precise and adequately substantiated notic**es, 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').

By requiring the provision of personal data in all cases of illegal content reporting, users are effectively obliged to disclose personal data in every instance, regardless of the criminal law context or severity of the offense. In addition to data already collected as part of the reporting process (such as the user ID), users are legally required to provide their full name and an email address. Furthermore, users are not informed about alternative channels or representatives who could assist them in reporting illegal content, such as public authorities or Trusted Flaggers, nor are they informed about the possibility of legal representation. Such an option—for example, representation by a legal representative in cases of copyright infringement—is available in Facebook's reporting interface (as illustrated in Figure 1), but not in TikTok's reporting interface.

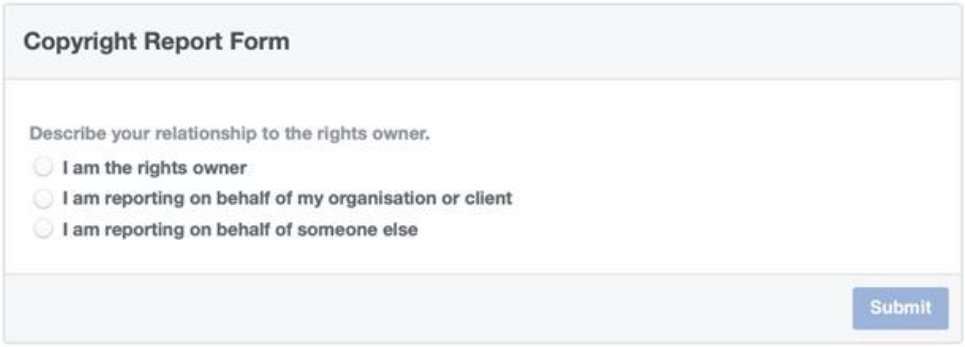


Figure 1 Facebook illegal content reporting mechanism interface for copyright infringement

This practice may conflict with the **principle of data minimization** under Article 5(1)(c) GDPR, as well as the requirements of data protection by design and by default set out in Article 25(1) GDPR. Such wide data collection design solutions increase the risk of de-pseudonymization, an issue of particular concern for marginalized or at-risk groups, such as individuals in repressive or authoritarian regimes, LGBTQ+ communities, or journalists.

The design of notice and action mechanisms varies across platforms in terms of how they define and categorize "illegal content." As Sekwenz et al. have found, Facebook (Meta) includes only four main categories of illegal content in its reporting interface, whereas TikTok distinguishes more than ten categories (see for this effect Figure 2 in this cited publication).[21]

The design of input fields on Facebook also varies depending on the selected category of illegal content. For example, cases related to privacy or GDPR violations require different user input information compared to the broader "Other" category, which encompasses all

2025 ACM Conference on Fairness, Accountability, and Transparency (Association for Computing Machinery 2025) <https://dl.acm.org/doi/10.1145/3715275.3732036> accessed 27 June 2025.

[21] ibid.

remaining types of illegal content—such as terrorist content, drug-related offenses, or incitement to violence (see Figure 3). Moreover, the design differs across Member States (see Figure 4): Facebook provides a dropdown menu for Austria, France, and Germany, listing between 11 and 23 specific legal norms for users to choose from, whereas users in other Member States are instead presented with open text fields for manual input (see Figure 3). **Such design choices—such as the use of open text fields—may also encourage user behavior that conflicts with the GDPR's data minimization principle, leading users to disclose more personal data in the reporting process than is necessary.**

Figure 3 Overview of Facebooks 'other' illegal content reporting category

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 "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**".

While we agree that the EDPB Guidelines on deceptive design patterns provide insights and definitions into dark patterns, we welcome the EDPB to consult the latest academic scholarship on the interpretation of "user autonomy" that is protected by the Article 25(1) of the DSA. Notably, these latest studies presented below provide new interpretation into the reasoning of the effects of dark patterns on users.

Three autonomy violation-types

Besides deception (defined above), other autonomy-violation types exist impacting user's autonomy, including *manipulation*, *material distortion or impairment*, that can hinder their ability to make conscious choices and protect their personal data. These prohibited different autonomy violation types **are not clarified neither in Article 25, nor Recital 67 of the DSA, and not even defined in the GDPR.** Therefore, these autonomy-violation types lack conceptual foundation. Consequently, the undefined space surrounding them might invite varying interpretations among platforms, designers, developers, regulators and policy-makers, each seeking to foreground and disambiguate the concept according to their own pursuits. We invite the EDPB to consider the the following academic article that defines the three "influence types" presented in the Article 25(1) of the DSA and Recital 67.This work articulates these concepts through an interdisciplinary analysis of autonomy definitions from the fields of Law and Human-Computer Interaction (HCI):

- *Understanding the scope of Article 25 of the DSA in regulating dark patterns.* Cristiana Santos, Sanju Ahuja, Nataliia Bielova, and Christine Utz. Dark patterns and deceptive design patterns: Conceptualising and systematising a key contemporary phenomenon. R. Gellert, C. Santos, & H. Schraffenberger (Eds.), Edward Elgar. (2025, forthcoming). Link

Manipulation. Manipulation introduces a steering effect on user's choices and decisions, *manipulate* users "*to act for reasons [they] can't recognise*".[22] For example, Recital 67 DSA prohibits the presentation of choices in a non-neutral manner (also called "False Hierarchy"[23]) that has a "*steering effect on users and may unreasonably bias them towards the more prominent choice"*[24]. This design practice constitutes a form of manipulation, and cannot be considered deceptive.

Material distortion or impairment. Distortion or impairment intends to have a forcing or coercive effect on user's actions; or users are prevented from taking an action that they willingly want to take. "Recital 67 prohibits "*making certain choices more difficult or time-consuming than others*" (also called "Obstruction'') and "*repeatedly requesting a recipient of the service to make a choice where such a choice has already been made*" (also called "Nagging"). These practices are not deceptive, as there is no element of falsehood in either. They are also not manipulative, because they do not steer users as much as constrain them. They largely have a *forcing or coercive* effect, where a user acts unwillingly or involuntarily for reasons they can actually recognize or is prevented from taking an action that they willingly want to take. In "Obstruction", the user is discouraged from taking the more difficult or time-consuming course of action and unwillingly makes the easier choice. Regarding "Nagging", the user unwillingly makes a choice intended by a product or a service to avoid

[22] Daniel Susser, Beate Roessler, and Helen Nissenbaum, Technology, autonomy, and manipulation. Internet Policy Review, 8(2), (2019), https://doi.org/10.14763/2019.2.1410

[23] Colin M. Gray et al., An Ontology of Dark Patterns: Foundations, Definitions, and a Structure for Transdisciplinary Action (n 8), pp. 17-20. https://dl.acm.org/doi/10.1145/3613904.3642436

[24] See p. 7 of "Understanding the scope of Article 25 of the DSA in regulating dark patterns." Cristiana Santos, Sanju Ahuja, Nataliia Bielova, and Christine Utz. Dark patterns and deceptive design patterns: Conceptualising and systematising a key contemporary phenomenon. R. Gellert, C. Santos, & H. Schraffenberger (Eds.), Edward Elgar. (2025, forthcoming). Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4899559

repeated interruptions during a task that they are focused on. In each case, the user unwillingly makes a choice due to a set of constraints placed upon them, which impairs free choice without the use of deception and manipulation."

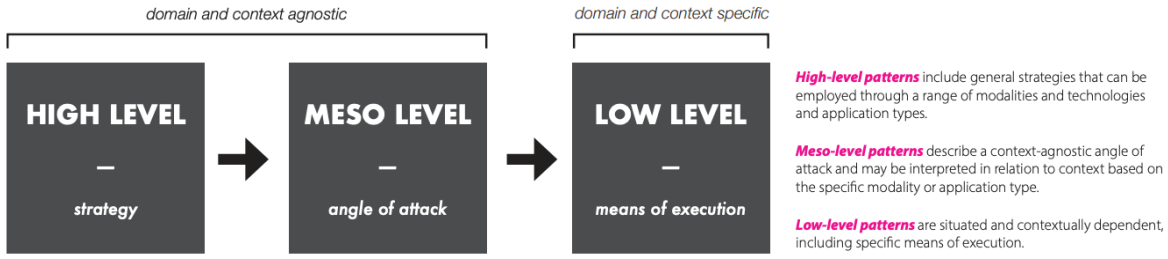
Combination of autonomy violation types. Some practices may constitute a combination of these influence types. We give a concrete example of such interplay of manipulation and distortion in the case of *Autoplay* below.

Mapping dark patterns to the Ontology of Dark Patterns knowledge

Multiple research groups have worked to systematize the knowledge around dark patterns. In parallel, regulators also issued their own guidance and reports on dark patterns. Several dark pattern types of these reports *overlap* in varying levels with dark pattern types from academic scholarship. We invite the EDPB to consider the following work[25] **that systematizes the knowledge and understanding of the various dark pattern** types in digital systems to avoid inconsistencies, gaps, or misalignment between academic knowledge and regulatory guidance.

- *An Ontology of Dark Patterns: Foundations, Definitions, and a Structure for Transdisciplinary Action.* Colin M. Gray, Nataliia Bielova, Cristiana Santos and Thomas Mildner. ACM CHI conference on Human Factors in Computing Systems (CHI), 2024. https://doi.org/10.1145/3613904.3642436

This scientific publication has rigorously analyzed **a total of 262 dark pattern type definitions**, drawing from **five major academic taxonomies**, as well as **five regulatory reports,**[26] including the EDPB guidelines on dark patterns. We invite the EDPB to base its reasoning about dark patterns on this **unified ontology which synthesizes 65 dark patterns types** across different levels of granularity: **low-, meso-, and high-level** patterns:



Levels of pattern granularity. From https://ontology.darkpatternsresearchandimpact.com/wp-content/uploads/2024/05/2024_Grayetal_CHI_OntologyReferenceSheet.pdf

[25] This ontology is cited by the Spanish Data Protection Authority (AEPD) report on addictive patterns in 2024, (https://www.aepd.es/guides/addictive-patterns-in-processing-of-personal-data.pdf). The ontology has been adopted and is currently being applied in three active regulatory cases at the EU Commission level involving several online platforms. This work accumulated a total of 150+ citations.

[26] (1) Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them. European Data Protection Board. 2023. Technical Report Version 2.0. LINK; (2) Behavioural study on unfair commercial practices in the digital environment : dark patterns and manipulative personalisation : final report. 2022. EU Commission. Publications Office of the European Union. LINK; (3) Dark commercial patterns. OECD Committee on Consumer Policy. Technical Report. 2022. LINK; (4) Evidence review of Online Choice Architecture and consumer and competition harm. UK CMA. Technical Report. 2022 LINK; (5) Bringing Dark Patterns to Light Staff Report. Technical Report. Federal Trade Commission. FTC Staff Report. 2022. LINK

The proposed ontology of dark patterns knowledge has therefore the following hierarchical structure that facilitates the understanding at three levels

- *High*: captures the overall strategy,
- *Meso*: identifies the angle of attack on the user,
- *Low:* specifies the concrete means of execution, thus manipulating, steering or impairing the user.

High-Level Pattern	Meso-Level Pattern	Low-Level Pattern
Obstruction D: Gr Lu Ma Br23 EUCOM FTC OECD I: EDPB CMA	Roach Motel (D: Br Gr Lu EUCOM I: Br23 Ma FTC OECD)	Immortal Accounts (D: Bö Lu FTC OECD)
		Dead End (D: EDPB)
	Creating Barriers	Price Comparison Prevention (D: Br Gr Lu FTC EUCOM OECD; I: Br23)
		Intermediate Currency (D: Gr Lu FTC EUCOM OECD; I: CMA)
	Adding Steps (I: EDPB)	Privacy Maze (D: EDPB)

Fragment of an ontology of dark patterns. From https://ontology.darkpatternsresearchandimpact.com/wp-content/uploads/2024/05/2024_Grayetal_CHI_OntologyReferenceSheet.pdf

Reasoning necessary to articulate why an observed design practice constitutes a specific autonomy violation type

Demonstrating such regulatory violations, however, requires **design-oriented reasoning** necessary to articulate why an observed design practice constitutes a specific autonomy violation type. We invite the Commission to consider the framework provided by an academic paper that maps 59 dark patterns from the dark patterns ontology (only meso- and low-level patterns) onto the three autonomy violation types from the DSA, and identifies **eight new design factors which can help determine when a dark pattern violates user autonomy**:

- *Dark Patterns and the EU Digital Services Act: Mapping Autonomy Violations and Design Factors.* Sanju Ahuja, Johanna Gunawan, Nataliia Bielova, Cristiana Santos. 2025. LINK

The **eight identified design factors** impact user decision-making through the:

- *Information Space*, i.e., all the information made available to the user by an online platform to support user choices and decisions, and
- *Choice Space,* i.e, the set of choices and options made available to the user by the online platform.

The detailed description of each space and factors can are provided in the publication. We believe these factors can assist the Commission in reasoning about dark patterns and violations of user autonomy and decision-making.

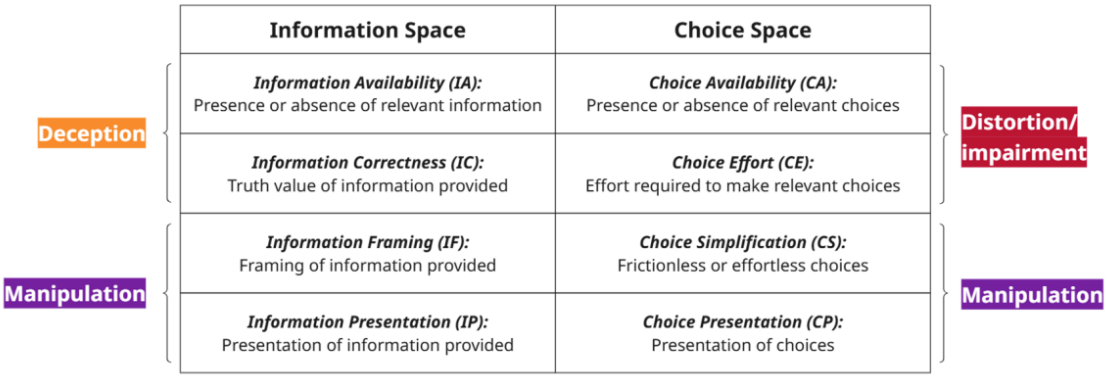


Fig. 4. Design factors which help determine the dark pattern autonomy violation type(s)

The following extract illustrates the reasoning developed in this paper:

> Pay-to-Play constitutes deception as it omits information (factor *IA*) or provides false or misleading information (factor *IC*) to create a false perception that a certain functionality of a product or a service is available via purchase or download, whilst later charging users additionally for that functionality.

Note that **one dark pattern practice can also constitute multiple autonomy violations types**, and can also produce additional effects on the user depending on the specific context. In such cases, all such reasoning is included, for example:

> Sneak into Basket constitutes distortion and deception. There is distortion/impairment as it constrains user choices by adding items to users' cart without any user action, whereas removal of these items necessitates direct action (factor *CA*). There is deception as it omits explicit information that such items have been added (factor *IA*).
> ***Additional autonomy violation:*** There is also a possibility of manipulation if it steers users towards a purchase through last minute presentation of potentially tempting items in the cart (factor *CP*) and the reduced friction in adding them to cart (factor *CS*).

We also invite the Commission to consider a recently published **methodology for capturing the potential and actual impacts of dark patterns over time**, referred to as the ''*Temporal Analysis of Dark Patterns*.'' This approach enables the assessment of how design practices evolve and how their effects on user autonomy may change over time.

- *Getting Trapped in Amazon's 'Iliad Flow': A Foundation for the Temporal Analysis of Dark Patterns.* Colin M. Gray, Thomas Mildner, and Ritika Gairola. 2025. In CHI '25: CHI Conference on Human Factors in Computing Systems Proceedings. LINK

This methodology enables expert evaluation of the presence of dark patterns through a disciplined and rigorous method. The evaluation approach utilizes the unified ontology across three scales:

– **intra-page**, which captures interactions on a single screen;

- **inter-page**, which captures interactions across two or more screens as a user seeks to accomplish their goal; and
- **system level**, which captures multiple touchpoints as a user engages with a system over time.

On purpose or effect

Recital 67, and by extension Article 25, covers autonomy-based violations that occur either *on purpose or in effect*. These provisions, however, do not provide a definition of what constitutes *on purpose* or *in effect*. Similarly, the EDPB guidelines on deceptive design patterns do not provide clarification on these concepts. We therefore invite the EDPB to consider the following proposed definitions:

On purpose includes practices (deception, manipulation, impairment/distortion) that are intentionally and deliberately aimed and used by an online platform, regardless of any actual demonstrable, observable effect or impact on its recipients. We deduce intentionality from the strategy of a platform and the predictable impact of the strategy, as follows:

- *Strategy:* the strategy that online platforms adopt by using a specific design practice directed at the recipients of their services. Specifically, the use of dark pattern practices in their online interfaces is a strategy adopted by an online platform to deceive, manipulate or impair user's autonomous choices and decisions;
- *Predictable impact of the strategy*: The online platform is aware of the reasonable likelihood that the adopted dark pattern strategy leads to a specific impact, such as increase in monetary income, increased consent rates, increased amount of collected data, higher rate of addiction of the recipients, etc.

The effect, orthogonally to intentionality, can be described as the unintended and unexpected consequence(s) for users as a result of their interaction with the specific dark pattern integrated in the online platform. The *in effect* statement holds even if a given practice was integrated without an anticipated purpose or strategy.

Method to determine whether an observed practice is in potential violation of the DSA under Article 25 and Recital 67

According to Art. 25(3) DSA, the Commission may issue guidelines on how Art. 25(1) DSA applies to specific practices. We propose the method to determine when dark pattern practices are in potential violation with the DSA, presented in the following publication:

- *Understanding the scope of Article 25 of the DSA in regulating dark patterns.* Cristiana Santos, Sanju Ahuja, Nataliia Bielova, and Christine Utz. Dark patterns and deceptive design patterns: Conceptualising and systematising a key contemporary phenomenon. R. Gellert, C. Santos, & H. Schraffenberger (Eds.), Edward Elgar. (2025, forthcoming). Link

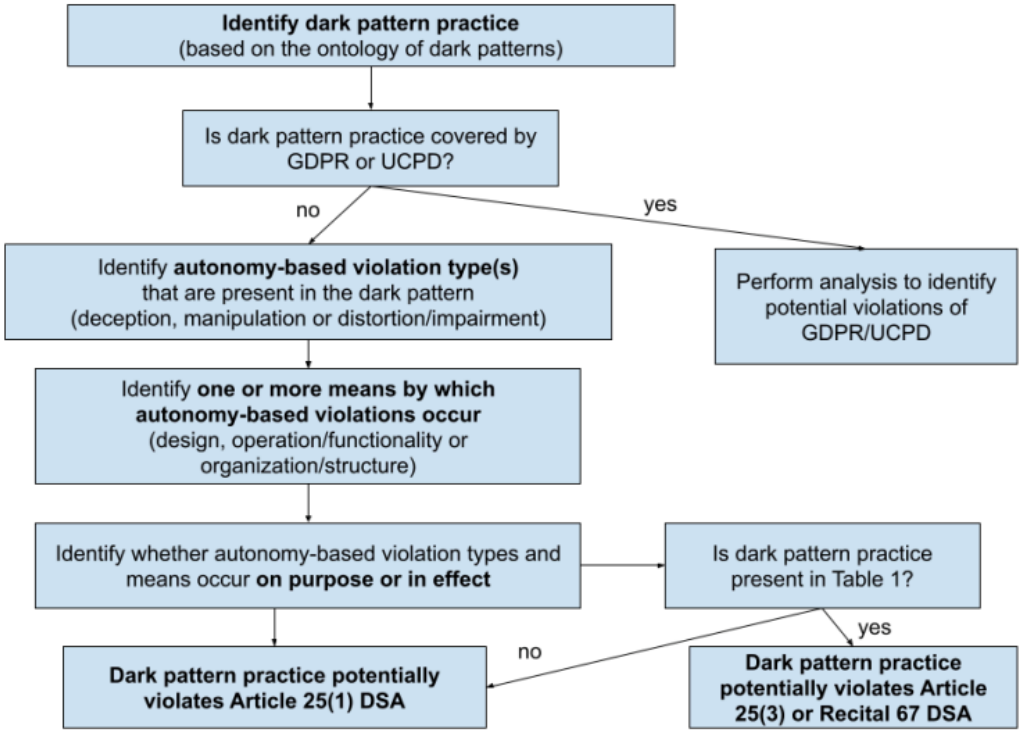


Figure 1. Method to determine when dark pattern practices are in potential violation with the DSA.

We suggest that the EDPB in its guidelines considers the following iteration.

1. First identify the dark pattern practice that is described in the unified ontology of Gray et al.[27] This unified ontology contains examples and complete definitions of each dark pattern type, against which the expert can evaluate the specific practice or user interface of a given online platform.
2. The next step is to identify whether the dark pattern practice could be subject to the GDPR (see our comments on this regard in the next section).
3. Then, for a given practice, we propose to identify the type or multiple types of autonomy-based violations present, such as deception, manipulation, or material distortion/impairment. The criteria for this mapping to autonomy violations are summarised as follows: (a) if a design practice "induces false beliefs either through affirmative misstatements, misleading statements, or omissions", it is mapped to *deception*; (b) if it has a steering effect in a certain direction, but without inducing false beliefs, and without coercing or constraining the user, it is mapped to *manipulation*; and (c) if the source of influence is coercion or a set of constraints placed upon the user's choice set, it is mapped to *material distortion and impairment*.
4. As also discussed in this same section, some design practices can be constituted by more than one influence-types. If a given dark pattern practice can be mapped to the ontology of Gray et al.[28], their autonomy violation(s) may be identified using the

[27] This ontology is cited by the Spanish Data Protection Authority (AEPD) report on addictive patterns in 2024, (https://www.aepd.es/guides/addictive-patterns-in-processing-of-personal-data.pdf). The ontology has been adopted and is currently being applied in three active regulatory cases at the EU Commission level involving several online platforms. This work accumulated a total of 150+ citations.

[28] This ontology is cited by the Spanish Data Protection Authority (AEPD) report on addictive patterns in 2024, (https://www.aepd.es/guides/addictive-patterns-in-processing-of-personal-data.pdf). The ontology has been

recent work of Ahuja et al.[29] These works map the known ontology dark patterns to the three autonomy violation types, along with providing justifications for each mapping – making it easier to connect these known practices to legal provisions.

5. Once autonomy-based violation type(s) are identified, the expert identifies the means by which the violation type(s) have occurred, such as *design, organisation /structure*, or *operation/functionality* of the online interface. In principle, each of the three influence-types can be operationalized in an online interface using different types of design elements (from a human-computer interaction lens). For a given practice, this mapping makes explicit what type of design elements have been used by the online interface to operationalise the identified influence-types.
6. After the autonomy-based violation type(s) and the means of such violations are identified, the expert analyses whether these violations occur *on purpose* or *in effect* (as explained above). This step includes a justification of whether the practice appears to be used intentionally and deliberately by an online platform (on purpose); or whether there is no appearance of an anticipated purpose or strategy but still there are unintended and unexpected consequence(s) for users (in effect).

If all steps have been followed and the corresponding autonomy-based violation types, their means and causes have been identified, then the observed practice potentially violates Article 25(1) and/or Recital 67. If the observed dark pattern practice is present in Table 1 and can be subsumed under one or more of the prohibited practices, then the analysed dark pattern practice also potentially violates Article 25(3) and/or Recital 67 (depending on which prohibited practice it maps to, according to Table 1).

In sum, we believe the definition of autonomy violations, ontology, design factors framework, and methodology for assessing the temporal analysis of dark patterns can be useful for the EDPB in their reasoning about Article 25(1).

Advertising practices not constituting dark patterns

Recital 67 DSA, which interprets Article 25, reads as follows: ‘’***Legitimate practices, for example in advertising,*** *that are in compliance with Union law* ***should not in themselves be regarded as constituting dark patterns****. Those rules on dark patterns should be interpreted as covering prohibited practices falling within the scope of this Regulation to the extent that those practices are not already covered under Directive 2005/29/EC or Regulation (EU) 2016/679.*’’ This formulation is problematic and requires further clarification. As formulated, this means that persuasive practices, such as advertising, are not in themselves considered dark patterns. As the EDPB posits in its own guidelines 08/2020 (paragraph 12), advertising (and targeting through advertising) can cause a risk of potential manipulation of users in terms of their purchasing decisions as consumers, or in terms of their political decisions as citizens engaged in civic life. While the DSA contains an adequate portfolio of provisions on transparency issues on online advertising, it fails to address targeted online manipulation through advertising. Neither Recital 67 nor Article 25 limit the micro-targeted online

adopted and is currently being applied in three active regulatory cases at the EU Commission level involving several online platforms. This work accumulated a total of 150+ citations.

[29] Sanju Ahuja, Johanna Gunawan, Nataliia Bielova, Cristiana Santos. *Dark Patterns and the EU Digital Services Act: Mapping Autonomy Violations and Design Factors,* 2025.https://hal.science/hal-05301214v1/document

manipulation through Adtech. Not all (if any) advertising is legitimate as of today, and persuasive practices can also be harmful/considered dark patterns. Research confirms that **algorithmic persuasion can manifest as online behavioral advertising.** Algorithmic persuasion operates at scale by inferring consumers' characteristics such as demographic, psychological characteristics and personalizing content accordingly. Such personalization is aimed at increasing one's susceptibility to influence. Empirical research shows that algorithmic persuasion produces a range of harms that extend beyond deception or financial loss. These systems, by continuously personalizing and optimizing persuasive content, can undermine autonomy, well-being, cognitive capacity, and emotional states. This raises questions about **manipulative potential, consumer autonomy, and the limits of legitimate commercial influence. Consumer vulnerabilities can be targeted for the purposes of personalized advertising and pricing as key harms to consumer welfare. We suggest that the EDPB clarify when advertising practices impairing user autonomy can nonetheless be considered dark patterns.** See on this regard the following academic works:

- The exploitation of vulnerability through personalised marketing communication: Are consumers protected? Joanna Strycharz, Bram Duivenvoorde (2021), Internet Policy Review, ISSN 2197-6775, Alexander von Humboldt Institute for Internet and Society, Berlin, Vol. 10, Iss. 4, pp. 1-27 Link
- The harmful side of algorithmic persuasion: A systematic review on the conceptualization of non-material harms. Wang, Y., Strycharz, J., Meppelink, C. S., Voorveld, H. A. M. (2025). Paper presented at the 23rd International Conference on Research in Advertising (ICORIA) 2025, Rotterdam, Netherlands.
- The algorithmic persuasion framework in online communication: conceptualization and a future research agenda. Zarouali, B., Boerman, S. C., Voorveld, H. A., & van Noort, G. (2022). Internet Research, 32(4), 1076-1096. Link

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.

Interplay between Article 25(2) of the DSA and GDPR

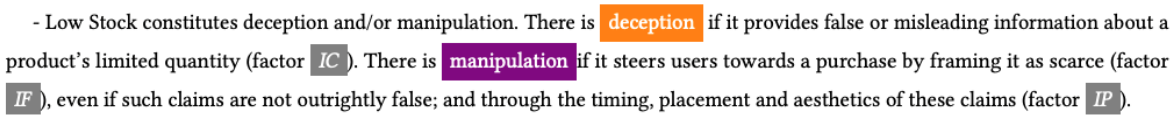
The EDPB should include the influence on all decisions related to the processing of non-personal data, in particular the data of legal persons as well as machine data. Key elements to consider when assessing whether a deceptive design pattern is covered by the GDPR are whether (i) ''*personal data is being processed*'', and (ii) ''*the data subject's behaviour that the pattern is influencing relates to the processing of personal data*''. **Criteria (i) "personal data processing"** might limit the fact that dark patterns operate prior to or independently of identifiable personal data collection. *Misleading defaults* may not *yet* involve "processing" personal data as defined in Article 4(2) GDPR, but it has the potential to significantly impact the users' ability to make autonomous and freely given choices regarding such processing. Such designs already undermine the principle of fairness (Article 5(1)(a)), **even before** personal data processing occurs. Thus, a purely processing-based test risks excluding dark patterns that are nonetheless relevant to the GDPR's protective aims. **Criteria (ii) ''the data subject's behaviour that the pattern is influencing relates to the processing of personal data''** does not offer sufficient interpretation about when a behaviour is "related enough" to personal data processing to trigger GDPR application. This is the more serious since dark patterns may affect user choices in subtle, cumulative ways that are difficult to evidence. We invite the EDPB to provide examples and guidance on two tests given to trigger the application of the GDPR.

Example given on low stock

We believe the example "**There are only a few products left in stock**" corresponds to a low-level dark pattern "*Low Stock*", defined in the ontology of dark patterns presented above as:

"*Low Stock* uses *Social Proof* as a type of *Social Engineering* to indicate that a product is limited in quantity, even though that claim is misleading or false. As a result, the user may assume that a product is desirable due to demand, leading to undue or uninformed pressure to buy the product immediately."

Moreover, expert reasoning about each dark pattern presented in the paper mentioned above (*Dark Patterns and the EU Digital Services Act: Mapping Autonomy Violations and Design Factors*), concludes that this dark pattern can present two autonomy violation types: deception and manipulation from Article 25(1):


- Low Stock constitutes deception and/or manipulation. There is deception if it provides false or misleading information about a product's limited quantity (factor IC). There is manipulation if it steers users towards a purchase by framing it as scarce (factor IF), even if such claims are not outrightly false; and through the timing, placement and aesthetics of these claims (factor IP).

Reasoning about "Low Stock" dark pattern — see p. 38 of https://hal.science/hal-05301214v1/document

The false information about a limited quantity leads to the user's **deception**, while the dark pattern employs the design factor "Information Correctness" (IC) that is concerned with the truth value of information provided. It also **manipulates** the user towards a purchase using the "Information Framing" (IF) design factor, but also relies on aesthetics of the claims, and hence the design factor "Information Presentation" (IP) is involved. This reasoning shows that the mere statement "**There are only a few products left in stock**" may already violate the Article 25(1) of the DSA.

The second example "**There are only a few products left in stock. Enter your email address now and make a reservation**", however, consists of the first statement, and an additional steering towards providing personal data. We suggest that, while the second statement "**Enter your email address now and make a reservation**" indeed is subject to the GDPR, the first part of the statement is still deceptive and manipulative (as discussed above) and the DSA should still apply to this case.

> 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 "***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]

User studies to be considered in the assessment of fairness

In the assessment of fairness, and to consider the legitimate expectations of data subjects, we recommend the EDPB to consider the following user studies on dark patterns.

While adults have the theoretical capacity to detect dark patterns and and resist their effects, this is very hard to achieve in practice. A recent empirical study demonstrates that **adults cannot easily resist to digital deception** due to several reasons included **human inherent bounded rationality** and that, even those that are highly aware of the possibility of being manipulated and that are capable of recognizing deceptive attempts are not necessarily better equipped to resist them:

- *I am Definitely Manipulated, Even When I am Aware of it. It's Ridiculous!" - Dark Patterns from the End-User Perspective.* Bongard-Blanchy K, Rossi A, Rivas S, et al. In: Designing Interactive Systems Conference (ACM DIS'21), see pp. 772-773, https://dl.acm.org/doi/10.1145/3461778.3462086

Children are particularly vulnerable to dark pattern exposure since their cognitive defenses are still developing. In a recent study, we draw on **abundant evidence** to demonstrate that anyone can be vulnerable to dark patterns, but some individuals or groups maybe more severely harmed than others because of multiple factors that we identify (ranging from age and digital literacy to socio-economic conditions). In this academic publication, we also critically discuss the extent to which the GDPR, the DSA and the AI Act are apt to integrate such a multi-layered model of vulnerability within their risk assessment methods:

- *Who is vulnerable to deceptive design patterns? A transdisciplinary perspective on the multi-dimensional nature of digital vulnerability*. Rossi A, Carli R, Botes MW, et al. Computer Law & Security Review 55:106031, 2024. LINK

Other recent research articles show that **children can only recognize around 30% of dark patterns**.[30] This leads to a particularly high exposure to persuasive, profit-driven tactics aimed at children.

[30] René Schäfer et al., *Fighting Malicious Designs: Towards Visual Countermeasures Against Dark Patterns* (CHI '24, ACM, 2024), https://doi.org/10.1145/3613904.364266; Carla Sousa and Ana Filipa Oliveira, *The Dark Side of*

Another user study on vulnerable users confirmed that **being aware of manipulative design does not automatically give users effective resistance**. Users in vulnerable situations often face more friction, less support, fewer alternatives when manipulation occurs, which amplifies negative outcomes. Manipulative design is often experienced as "normal" by users, undermining their ability to question or resist. The interplay of user skills, context, design, business model and system affordances matters: regulators can't consider the user in isolation:

- Lorena Sánchez Chamorro. 2025. *Resisting the 'Matrix': Perceptions of Manipulative Designs Among Vulnerable Users.* Proc. ACM Hum.-Comput. Interact. 9, 7, Article CSCW471 (November 2025), 31 pages. https://doi.org/10.1145/3757652

The user study of Mildner et al. highlight several key points that matter most for regulators. Regulatory guidelines should include usability and accessibility standards for exercising rights (deletion, consent, settings).

- Thomas Mildner, Gian-Luca Savino, Susanne Putze, and Rainer Malaka. 2024. *Finding a Way Through the Social Media Labyrinth: Guiding Design Through User Expectations.* In Proceedings of the International Conference on Mobile and Ubiquitous Multimedia (MUM '24). Association for Computing Machinery, New York, NY, USA, 157–171. https://doi.org/10.1145/3701571.3701605

Fairness beyond transparency

The EDPB rightly affirms that deceptive design patterns are generally unlawful under Article 5(1)(a) GDPR, and that fairness is an overarching principle requiring data not be processed in ways that are detrimental, discriminatory, unexpected, or misleading. However, to operationalize this principle effectively, guidance is necessary and must go beyond transparency: it must address **fairness as a systemic condition for autonomy** in digital environments. The transparency-enhancing best practices (such as clear language, accessible controls, and improved interface design) proposed in the EDPB's Guidelines 03/2022 play a crucial role in enabling users to understand their rights and make informed choices. Yet, these practices act locally on the user interface and **do not address the broader conditions that shape user behavior**. The EDPB's emphasis on transparency in the 03/2022 Guidelines probably derives from the conceptualization of deceptive design patterns as practices that "can hinder [users'] ability to effectively protect their data and make conscious choices" by nudging users "into making unintended, unwilling and potentially harmful decisions [...] regarding the processing of their personal data" (p. 3). Albeit not factually wrong, the definition is ill-formed: individuals are often unable to protect their data because a complex set of factors renders them vulnerable; what is more, the **striving towards conscious decision-making may be unreasonable**, and actually harmful. Deceptive design patterns exploit not only informational asymmetries but also users' bounded rationality, emotional states (e.g., stress, fatigue), and socio-economic vulnerabilities, including digital literacy

Fun: Understanding Dark Patterns and Literacy Needs in Early Childhood Mobile Gaming (Proceedings of the 17th European Conference on Games Based Learning, 2023), https://doi.org/10.34190/ecgbl.17.1.1656

gaps.[31] In such contexts, **transparency may reveal unfair practices but cannot prevent them**, especially when users lack the capacity, time, or motivation to engage with complex privacy decisions.

Moreover, manipulative designs often operate **below the surface of the graphical UI**, in back-end data flows that remain invisible to users. Studies show that consent management platforms disregard opt-out choices, mobile apps share data with third-party trackers despite user preferences, and IoT devices transmit intimate data without meaningful consent. These practices undermine user control and autonomy, regardless of how transparent the interface may appear. Fairness, by contrast, addresses the structural power asymmetries that transparency alone cannot resolve. It requires organizations to adopt **accountable practices**, such as data minimization and privacy by design and default, and regulators to align enforcement across data protection, consumer, and competition law. For example, mechanisms like data portability and interoperability (enshrined in the GDPR, DMA, and Data Act) are essential to counter lock-in effects and support user agency. However, **these rights are only meaningful when embedded in a fair environment** that enables users to act on their preferences without undue constraints.

The conceptualization of fairness proposed by Clifford and Ausloos [32] underscores its procedural role: organizations must demonstrate accountability of fairness not only through transparent disclosures but by ensuring that their data practices are substantively fair. This includes balancing business interests with the real and present interests of individuals, and considering the *expectations* of data subjects in context. **Without guidance on how to achieve this, fairness remains a principle in theory** but not in practice.

Furthermore, the design of digital environments is shaped by complex organizational decisions at the operational, business, and infrastructural levels that often fall outside the remit of data protection authorities. To recommend fair design patterns, we must **understand why certain patterns are adopted, clarify responsibilities across the data supply chain, and develop economic incentives that go beyond compliance**. A regulatory focus on transparency-enhancing UI elements, while valuable, does not address the deeper systemic incentives that perpetuate manipulative practices.

Fairness also plays a foundational role in enabling autonomy. It creates the conditions for users to exercise freedom of choice, make decisions based on trustworthy grounds (agency), oversee system behavior (control), trust their environment (self-constitution), and avoid exploitation of cognitive biases (independence). These dimensions of autonomy cannot be supported by transparency alone. In conclusion, while transparency is necessary, it is not sufficient. To effectively counter deceptive design patterns and support autonomous decision-making, we urge **the EDPB must provide concrete guidance on how to realize fairness in practice**. This includes systemic interventions, organizational accountability, and

[31] Weprovide a clear list of evidence-based vulnerability factors in: Rossi, A., Carli, R., Botes, M. W., Fernandez, A., Sergeeva, A., & Sánchez Chamorro, L. (2024). Who is vulnerable to deceptive design patterns? A transdisciplinary perspective on the multi-dimensional nature of digital vulnerability. Computer Law & Security Review, 55, 106031. https://doi.org/10.1016/j.clsr.2024.106031

[32] Clifford, D., & Ausloos, J. (2018). Data Protection and the Role of Fairness. Yearbook of European Law, 37, 130–187. https://doi.org/10.1093/yel/yey004

incentive structures that promote fair design choices. Without fairness, **transparency risks becoming a superficial fix in a structurally imbalanced system.**

We have addressed such concerns more in detail in the following publication:

- Arianna Rossi, "A fair digital environment was not built in a day: on the reasons why bolstering autonomous decision-making must go beyond UI design recommendations" Dark patterns and deceptive design patterns: Conceptualising and systematising a key contemporary phenomenon. R. Gellert, C. Santos, & H. Schraffenberger (Eds.), Edward Elgar. (2025, forthcoming).

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.

Attention Capturing Design Practices (ACDPs)

Recent research proposed a systematic literature review conceptualising *''Attention Capture Deceptive Patterns'' (ACDPs)*: these patterns are defined as "*recurring pattern[s] in digital interfaces that a designer uses to exploit psychological vulnerabilities and capture attention, often leading the user to lose track of their goals, lose their sense of time and control, and later feel regret*" (see section 3.1 of the publication). We encourage the Commission to consider this work on ACDPs in its assessment of dark patterns and their impact on user autonomy:

- *Defining and Identifying Attention Capture Deceptive Designs in Digital Interfaces.* Alberto Monge Roffarello, Kai Lukoff, and Luigi De Russis. 2023 CHI Conference on Human Factors in Computing Systems (CHI '23). LINK
- Hao-Ping (Hank) Lee, Yi-Shyuan Chiang, Lan Gao, Stephanie Yang, Philipp Winter, and Sauvik Das. 2025. *Purpose Mode: Reducing Distraction through Toggling Attention Capture Damaging Patterns on Social Media Web Sites.* ACM Trans. Comput.-Hum. Interact. 32, 1, Article 10 (February 2025), 41 pages. Link
- Kai Lukoff, Ulrik Lyngs, Himanshu Zade, J. Vera Liao, James Choi, Kaiyue Fan, Sean A. Munson, and Alexis Hiniker. 2021. *How the Design of YouTube Influences User Sense of Agency.* In Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI '21). Association for Computing Machinery, New York, NY, USA, Article 368, 1–17. Link

In this work, researchers analysed 98 academic publications on dark patterns and identified **11 ACDPs observed primarily in social media platforms**, but also present in games and video streaming services. Below is a fragment of the proposed ACDPs.

Table 4: A typology of 11 attention capture damaging patterns.

Pattern Name	Description	Main Context(s) of Use
P1 - Infinite Scroll	As the user scrolls down a page, more content automatically and continuously loads at the bottom.	Social media (e.g., Facebook, Instagram, and Twitter).
P2 - Casino Pull-to-refresh	When the user swipes down on their smartphone, there is an animated reload of the page that may or may not reveal new appealing content.	Social media on smartphones.
P3 - Neverending Autoplay	A new video is automatically played when the current one finishes. There is never a point for the user to stop and reflect, and the option to turn off autoplay is hidden or non-existent.	Social media and video streaming platforms, e.g., YouTube.
P4 - Guilty Pleasure Recommendations	Personalized suggestions that prey on individual consumer frailty to target user's guilty pleasures and increase use time.	Social media and video streaming platforms, e.g., YouTube.

Interestingly, researchers have further developed the analysis of how these patterns affect user autonomy, and proposed an extended **mapping of ACDPs** to the **autonomy violations** and **eight design factors** (already introduced above):

- *Dark Patterns and the EU Digital Services Act: Mapping Autonomy Violations and Design Factors.* Sanju Ahuja, Johanna Gunawan, Nataliia Bielova, Cristiana Santos. 2025. LINK

A fragment of the proposed mapping is presented below:

Design Practice	Definition	Ontology Mapping	Autonomy Violations and Design Factors
Casino Pull-to-refresh	When the user swipes down on their smartphone, there is an animated reload of the page that may or may not reveal new appealing content.	New low-level of *Attention Capture*^{M}	manipulation *Information Framing* IF: Steers users to spend more time by framing the upcoming content as 'novel' using animated reload *Choice Simplicification* CS: Steers users to spend more time by creating a frictionless refreshing experience which does not allow reflection over time spent
Neverending Autoplay	A new video is automatically played when the current one finishes. There is never a point for the user to stop and refect, and the option to turn of autoplay is hidden or non-existent.	Mathes with existing low-level *Auto-Play*^{L}	manipulation *Choice Simplicification* CS: Steers users to watch more videos by creating a frictionless viewing experience which does not allow reflection over time spent ***Additional autonomy violation:*** distortion/impairment *Choice Availability* CA, *Choice Effort* CE: If it constrains user choices by making it impossible or difficult to turn off auto-play deception *Information Availability* IA: If it omits or hides the option to turn off auto-play

Another recent work on **harms caused by dark patterns** that reviews 39 sources (12 policy reports and 27 academic studies), proposed a total of **20 types of harm** (individual and collective, material and non-material harms), shows that **addiction is a harm in itself:**

- *No harm no foul: how harms caused by dark patterns are conceptualised and tackled under EU data protection, consumer and competition laws*. Cristiana Santos, Viktorija Morozovaite, and Silvia De Conca. 2025. Information & Communications Technology Law (2025), 1–47. Link

This research confirms that **addiction is also conducive to other harms,** including Financial loss (e.g. through gambling), cognitive harms, as impacting mental and even physical well-being. It is frequently discussed as intertwined, almost blurred, with ''Loss of time'' and ''Loss of autonomy''. Addiction is indicated as a factor that turns an average consumer into a **vulnerable one.** Moreover, this systematic review of the literature indicates that addiction is almost unanimously conceptualized as the combination of dark patterns. The possibility for redress is only dictated and limited by national courts and national tort liability regimes.

In sum, we believe this work of the academic community on evaluating the effect of autoplay, the overall structuring the knowledge about Attention Capture Deceptive Patterns (ACDPs), their mapping to autonomy violations, and the qualification of addiction as a harm in itself could be useful for the EDPB.

> 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]

Autoplay in online streaming services

Within online streaming services, several types of **autoplay** significantly affect the time spent on online services, and will likely have a particularly strong effect on minors. We invite the Commission to consider recent research that analysed different types of autoplay on Netflix.com and evaluated its impact on time spent:

- *An Experimental Study of Netflix Use and the Effects of Autoplay on Watching Behaviors.* B. Schaffner, Y. Ulloa, R. Sahni, J. Li, A.K. Cohen, N. Messier, L. Gao, M. Chetty. ACM Conference On Computer-Supported Cooperative Work And Social Computing (CSCW 2025). LINK

This academic research shown that there are various types of autoplay:

i. when **a piece of content ends, another piece automatically begins playing** (e.g., completing an episode on Netflix where another episode starts after 5 seconds),
ii. when **content automatically starts playing upon visiting a page or screen** (e.g., the `autopreview' that plays when first visiting Netflix.com, opening the app, or selecting a title for more information), and
iii. when **content automatically plays when a cursor or selector passes over it** (e.g., the `hoverplay' when a cursor or a smart TV selector passes over a thumbnail).

All three play a role in platforms designed to maximize engagement—with types (ii) and (iii) being the most prominent at the beginning of sessions ("hook"), and type (i) effectively extending sessions. Autoplaying promotional content (ii) and (iii) also plays a significant role in the choice of content that viewers ultimately watch.

This study showed that the majority of new viewings (i.e., starting a new show or movie) came after seeing a promotional content for that title. This recent work has **quantitatively demonstrated the potential powerful effects of content autoplaying one after another (i)**. Researchers found that in a controlled field-experiment on Netflix, **disabling autoplay decreased participants' daily watching by 21 minutes** and average session lengths by 18 minutes. On average, users waited 24 seconds longer between episodes, suggesting that making them play the next show themselves led to longer pauses and less total watching. When participants were asked to reflect on the experiment, their anecdotes signal increased awareness and control over their time: "[*Disabling autoplay] did make me realize how many episodes I was watching more so then as before. I didn't pay attention to it as much because it was automatic before*."

Another study conducted interviews with moderate heavy Netflix users in the US which gives further **qualitative insights into the potentially addictive behaviour of autoplay**:

- *Don't Let Netflix Drive the Bus: User's Sense of Agency Over Time and Content Choice on Netflix*. B. Schaffner, A. Stefanescu, O. Campili, M. Chetty. ACM Conference On Computer-Supported Cooperative Work And Social Computing (CSCW 2023). LINK

The **automatic playing of content puts participants in an opt-out, under-pressure, decide-later dynamic** instead of the alternative: opt-in, reflective, intentional sessions as their statements demonstrate: "*I actually am very opposed to autoplaying [...] whenever I finish a thing, I definitely want to stop, turn off the TV and take a break. But definitely I fall into like, 'Ah, this was so great. I should just watch one more episode. One more episode. It's not too late.' [...] And I don't appreciate that as a business decision to keep people engaged*."

This sentiment is reflected in the aforementioned work (*Dark Patterns and the EU Digital Services Act: Mapping Autonomy Violations and Design Factors*) mapping the Attention Capture Design Patterns — and specifically 'Neverending Autoplay' to the extant DSA autonomy violation types — deception, distoortion/impairment and deception — as identified by the work mentioned above (*Understanding the scope of Article 25 of the DSA in regulating dark patterns*):

Neverending Autoplay	A new video is automatically played when the current one finishes. There is never a point for the user to stop and refect, and the option to turn of autoplay is hidden or non-existent.	Mathes with existing low-level *Auto-Play*[L]	manipulation *Choice Simplicification* CS: Steers users to watch more videos by creating a frictionless viewing experience which does not allow reflection over time spent ***Additional autonomy violation:*** distortion/impairment *Choice Availability* CA, *Choice Effort* CE: If it constrains user choices by making it impossible or difficult to turn off auto-play deception *Information Availability* IA: If it omits or hides the option to turn off auto-play

We invite the EDPB to consult this works since the DSA's perspectives on infringements to user autonomy are already well-suited to tackling Attention Capture Design Patterns.

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**"

What the EDPB guidelines mean for children

The text in bold is confusing because this quote from Recital 71 merely provides background on what it means for a platform to be 'accessible to minors'. To the extent that Recital 71 refers to data processing for other purposes that provides awareness of age, the EDPB Guidelines should guide **how this relates to purpose limitation** (and specific considerations concerning processing personal data of children as vulnerable data subjects).

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.

The sentence "providers of online platforms should ensure a high level of privacy, safety and security for all its users" is confusing because it may imply to readers that 'high level of privacy, safety and security' is similar or the same for children and adults. It disregards that **children are often more vulnerable** than most adults. Instead, as the above general comments consider, **the EDPB Guidelines should specify what the GDPR means for *children* in the interplay with the DSA**.

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.**

It is necessary to add that behavioral profiling as age assurance, a method used by online platforms, is likely unlawful under the GDPR.[33]

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.

This paragraph states that a risk-based approach is necessary regarding age assurance, but the text is not entirely correct.The text provides: "*Take a risk-based approach when ensuring that minors cannot access the platform*." Preventing children from accessing a platform is not always necessary; sometimes, it is a matter of not giving them access to certain parts of the service or specific functionalities.

The text states follows: "*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*)". We have privacy-friendly methods that will, by design, limit personal data to what is necessary and proportionate. This should be acknowledged here (and not only in footnotes). Therefore, even in cases where an exact minimum (or maximum) age must be *verified* (and not merely an age range), it is unnecessary to provide a birth date. Moreover, one only knows with sufficient certainty whether a user is within a specific age range by

[33] R Shaffique, S van der Hof, Behavioural Profiling For Age Assurance: Do The Ends Justify The Means? International Data Protection Law Review (forthcoming 2025 / draft can be requested from the authors).

performing age verification. In that case, one can verify against the exact birth date, but it may be helpful to note that this information need not be disclosed. Hence, taking a risk-based approach to deciding on measures for online platforms to ensure a high level of privacy, safety, and security, age assurances as a *specific* mitigating measure can and should be privacy-friendly pursuant to Articles 5 and 25 of the GDPR.

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 sufficient to ask for confirmation that the user is above a relevant threshold and, in case of doubt, to carry out further checks120 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 GDPR121, but also, for example, from other instruments of EU or Member State law122. 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.

Regarding the bold text, if a service is low risk for children, then age assurance and processing personal data for that purpose are unnecessary; therefore, the necessity test will not be satisfied. If a (part of a) service is low risk for older children but high risk for younger children, age verification is necessary to ensure the younger age group does not have access. Still, as stated earlier, age verification can be done in a privacy-friendly way. The text also needs clarification with respect to 'further checks' and 'measures that benefit all users', because it is not entirely clear what they mean. Moreover, it may confuse readers when the guidelines address Articles 34 and 35 in the section on Article 28. These provisions should be discussed in Section 2.7, positioning age assurance as a potential mitigating measure to address systemic risks to children's fundamental rights, protection, and well-being, that must comply with the GDPR, particularly Article 25 GDPR.

2.7 Risk assessment and mitigation (Articles 34 and 35

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

Dark Patterns and Systemic Risk in Online Platform Design

If systemic risks are identified, a data protection impact assessment (DPIA) can inform how to test and manage them under the DSA, including evaluating the design of reporting systems. Research, such as that by Wagner et al.[34] has shown that similar design issues have already been observed under Germany's Network Enforcement Act (NetzDG). There, "nudging" or dark pattern design practices—such as long or complex reporting paths, unclear language, or hidden reporting options—were found to make reporting illegal content more difficult and to violate legal transparency requirements.

[34] Ben Wagner and others, 'Mapping Interpretations of the Law in Online Content Moderation in Germany' (2024) 55 Computer Law & Security Review 106054.